creative commons
COMMONS DEED

저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

이학석사 학위논문

Quantum zero-error capacity

(양자 무오류 용량)

2019년 8월

서울대학교 대학원

수 리 과 학 부

정 남 호

Quantum zero-error capacity

(양자 무오류 용량)

지도교수 이 훈 희

이 논문을 이학석사 학위논문으로 제출함

2019년 4월

서울대학교 대학원

수 리 과 학 부

정 남 호

정남호의 이학석사 학위논문을 인준함

2019년 6월

위 원 장 계 승 혁 인

부 위 원 장 이 훈 희 인

위 원 정 자 아 인

Quantum zero-error capacity

by

Namho Jeong

A DISSERTATION

Submitted to the faculty of the Graduate School
in partial fulfillment of the requirements
for the degree Master of Science
in the Department of Mathematics
Seoul National University
August 2019

Abstract

In these days, quantum information theory is rising up as one of the important tools in IT fields. Together with functional analysis, it could be more exquisite mathematically. Similarly to classical information theory, it is important to find out whether the input data is modified. In quantum version, it is a significant problem to examine reliability of some quantum channels where the input data pass through.

It turned out that each quantum channel corresponds to a mathematical structure called operator system. In this thesis, we focus on the operator systems associated with given channels and aim to find the value that indicates the reliability of the system. However, it is sometimes hard to compute the value depending on channels. Hence, we alternatively examine some upper bounds for the value. In Chapter 5, we examine several examples of quantum channels for computing those values, which are selected from the literature as well as some new ones.

Keywords : Quantum channel, independence number, Lovász theta function
Student number : 2014-21194

Contents

Chapter 1

Introduction

Claude E. Shannon proposed information theory in 1948, which studies the quantification, storage and communication of information. Since then, there have been a lot of studies about information theory using probability. Information is the most important resource in communications. In contrast to the past, people exchange their data or information through 'special' channels like quantum channels. But errors in communications can always happen, so it is important to find, at least, how much of reliable information at each channel can send without error which is called the zero-error capacity. Because every quantum channel corresponds to some operator system, we actually focus on the operator system corresponding to a given channel.

Chapter 2 provides preliminaries including elementary essential, elementary concepts for quantum communication. We begin to examine postulates and tools of quantum mechanics in Chapter 3. This chapter provides not only many new concepts but easier methods to compute independence number, which is our final goal. In Chapter 4, we can formalize an operator system from each graph. Note that the converse does not hold, that is, it is

not true that each operator system can always derive a graph. In the final chapter we introduce concepts of the zero-error communication where the outcome M is equal to the input information m with probability 1. With concepts acquired in Chapter 3, we examine its properties, and compute some values through several examples that indicate the reliability of each channel.

Throughout this thesis, we use the notations $\mathcal{H}, \mathcal{H}_{\mathcal{A}}, \mathcal{H}_{\mathcal{B}}, \mathcal{K}$ as Hilbert space, and we will assume that all Hilbert spaces in this thesis are finite dimensional.

Chapter 2

Preliminaries

2.1 Operator system

Our goal is to compute independence number of a channel, but it is difficult to find the value directly. So we use a alternative method, using "operator system". Recall that $\mathcal{B}(\mathcal{H})$ is a C^*-algebra whenever $\mathcal{H}$ is a Hilbert space. By definition, $\mathcal{B}(\mathcal{H})$ has naturally an involution, that is, a map $\mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$, defined by $X \mapsto X^*$. (X^* is the *adjoint* of X.)
Throughout this thesis, "$X \geq 0$" means that X is positive semidefinite whenever X is an operator.

Definition 2.1.1 A subspace $S \subseteq \mathcal{B}(\mathcal{H})$ is called an **operator system** if
(1) $1 \in S$
(2) If $X \in S$, then $X^* \in S$.

If S is an operator system, then $S_+ := S \cap \mathcal{B}(\mathcal{H})_+$ linearly spans S. (Here, $\mathcal{B}(\mathcal{H})_+ = \{X \in \mathcal{B}(\mathcal{H}) : X \geq 0\}$). To see this, for any hermitian element $a \in S$, the equality $a = \|a\| 1 - (\|a\| 1 - a)$ holds. Then the result follows from that for any element $X \in S$, $X = \frac{X+X^*}{2} + i\frac{X-X^*}{2i}$.

Note that for each Hilbert space $\mathcal{H}$, there is a natural identification between $M_n(\mathcal{B}(\mathcal{H}))$ and $\mathcal{B}(\mathcal{H}^{(n)})$, where $M_n(S) = \{[a_{ij}] : a_{ij} \in S, 1 \leq i, j \leq n\}$, $\mathcal{H}^{(n)} = \underbrace{\mathcal{H} \oplus \cdots \oplus \mathcal{H}}_{n-copies}$. Thus, if $S \in \mathcal{B}(\mathcal{H})$ is an operator system, then clearly so is $M_n(S) \subseteq \mathcal{B}(\mathcal{H}^{(n)})$.

2.2 Tensor product of matrices(Kronecker Product)

If $X : \mathcal{H} \longrightarrow \mathcal{H}$ and $Y : \mathcal{K} \longrightarrow \mathcal{K}$ are linear, then there is a well-defined linear map $(X \otimes Y) : \mathcal{H} \otimes \mathcal{K} \longrightarrow \mathcal{H} \otimes \mathcal{K}$ defined by $(X \otimes Y)(h \otimes k) = X(h) \otimes Y(k)$ for all $h \in \mathcal{H}$, $k \in \mathcal{K}$.
Particularly, for linear maps $T_1 : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ and $T_2 : \mathcal{H} \longrightarrow \mathcal{H}$, our goal in this subsection is to express a matrix representation of $T_1 \otimes T_2$. To do this, we have to pass through three steps.

STEP1. Find a natural identification of typical element in $\mathbb{C}^n \otimes \mathcal{H}$

If $\{e_1, \cdots e_n\}$ is a standard orthonormal basis of $\mathbb{C}^n$, then every element $v \in \mathbb{C}^n \otimes \mathcal{H}$ has a unique representation given by $v = \sum_{i=1}^n e_i \otimes h_i$, where $h_i \in \mathcal{H}$, and

$$\|v\|^2 = \langle \sum_{i=1}^n e_i \otimes h_i, \sum_{j=1}^n e_j \otimes h_j \rangle = \sum_{i,j=1}^n \langle e_i, e_j \rangle_{\mathbb{C}^n} \langle h_i, h_j \rangle_{\mathcal{H}}$$
$$= \sum_{i=1}^n \|h_i\|^2 = \|(h_1, \cdots, h_n)\|^2,$$

where $< \cdot, \cdot >$ is an inner product.

This means that we have the Hilbert space isomorphism

$$\mathbb{C}^n \otimes \mathcal{H} \simeq \underbrace{\mathcal{H} \oplus \cdots \oplus \mathcal{H}}_{n-copies}$$

via the natural identification $\sum_{i=1}^{n}(e_i \otimes h_i) \simeq \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix}$.

STEP2. Find a natural identification of a linear map in $\mathcal{B}(\mathbb{C}^n \otimes \mathcal{H})$

We can consider $A = (A_{ij}) \in M_n(\mathcal{B}(\mathcal{H}))$ as an operator defined by

$$A \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{n} A_{1j}h_j \\ \vdots \\ A_{nj}h_j \end{pmatrix} \in \underbrace{\mathcal{H} \oplus \cdots \oplus \mathcal{H}}_{n-copies}$$

Therefore, we obtain a natural identification $M_n(\mathcal{B}(\mathcal{H})) \simeq \mathcal{B}(\mathbb{C}^n \otimes \mathcal{H})$.(In fact, every linear operator on $\mathcal{B}(\mathbb{C}^n \otimes \mathcal{H})$ has such matrix representation)

STEP3. Find a matrix representation of $T_1 \otimes T_2$

As in the beginning of this subsection, assume that both $T_1 : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ and $T_2 : \mathcal{H} \longrightarrow \mathcal{H}$ are linear, and $T_1 = (a_{ij}) \in M_n(\mathbb{C})$. Then $T_1 \otimes T_2 : \mathbb{C}^n \otimes \mathcal{H} \longrightarrow \mathbb{C}^n \otimes \mathcal{H}$ has a matrix representation as an $n \times n$ block matrix in $M_n(\mathcal{B}(\mathcal{H}))$ whose entries are given by linear maps. Then

$$(T_1 \otimes T_2)(e_j \otimes h) = T_1(e_j) \otimes T_2(h) = \left(\sum_{i=1}^{n} a_{ij} e_i \right) \otimes T_2(h)$$

$$= \sum_{i=1}^{n} (e_i \otimes a_{ij} T_2(h)) \simeq \begin{pmatrix} a_{1j} T_2(h) \\ \vdots \\ a_{nj} T_2(h) \end{pmatrix} = (a_{ij} T_2) \begin{pmatrix} 0 \\ \vdots \\ h \\ \vdots \\ 0 \end{pmatrix},$$

where h is in the j-th position and 0 otherwise. The Kronecker product of T and R, is the block matrix $(a_{ij}T_2) \in M_n(\mathcal{B}(\mathcal{H}))$. Then we can know the followings :

1. there are n^2 blocks
2. each block has the size equal to $dim(\mathcal{H})$
3. (i, j)-block is $a_{ij}T_2$

As a result, we conclude that $T_1 \otimes T_2 = \begin{pmatrix} a_{11}T_2 & \dots & a_{1n}T_1 \\ \vdots & \ddots & \vdots \\ a_{n1}T_2 & \dots & a_{nn}T_2 \end{pmatrix}$, a block matrix with n^2 blocks, each of size $dim(\mathcal{H})$.

2.3 Complete positivity

Let $u : E \longrightarrow F$ be a linear mapping between operator systems E and F. Then for $n \geq 1$, $u_n : M_n(E) \longrightarrow M_n(F)$, defined by $u_n([a_{ij}]) = [u(a_{ij})]$

for all $[a_{ij}] \in M_n(E)$, is also a well-defined linear mapping between operator systems.

Definition 2.3.1 Let S be an operator system, and let $u : S \longrightarrow \mathcal{B}(\mathcal{K})$ be a linear mapping.

(1) u is said to be **positive** if for any $X \in S_+$, $u(X) \in \mathcal{B}(\mathcal{K})_+$.

(2) u is said to be n**-positive** if $u_n : M_n(S) \longrightarrow M_n(\mathcal{B}(\mathcal{K}))$ is positive.

(3) u is said to be **completely positive (CP)** if u is n-positive for all $n \geq 1$.

Example 2.3.2 Let $\Phi : M_p \longrightarrow M_p$ defined by $\Phi(X) = X^t$. We will show that Φ is positive but not 2-positive.

1. Φ is positive ;

   For any $X = (X_{ij}) \in M_p$, $X \geq 0$, and $\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_p \end{pmatrix} \in \mathbb{C}^p$,

$$\left\langle X^t \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_p \end{pmatrix}, \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_p \end{pmatrix} \right\rangle = \begin{pmatrix} \overline{\lambda_1} & \dots & \overline{\lambda_p} \end{pmatrix} X^t \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_p \end{pmatrix} = \sum_{i,j=1}^{p} \overline{\lambda_i}(X_{ij}^t)\lambda_j$$

$$= \sum_{i,j=1}^{p} \overline{\lambda_i}(X_{ji})\lambda_j = \sum_{i,j=1}^{p} \overline{\lambda_j}(X_{ij})\lambda_i = \sum_{i,j=1}^{p} \lambda_i(X_{ij})\overline{\lambda_j}$$

$$= \left\langle X \begin{pmatrix} \overline{\lambda_1} \\ \vdots \\ \overline{\lambda_p} \end{pmatrix}, \begin{pmatrix} \overline{\lambda_1} \\ \vdots \\ \overline{\lambda_p} \end{pmatrix} \right\rangle \geq 0,$$

which implies that Φ is positive.

2. Φ is *not* 2-positive;

   - $E = \begin{pmatrix} E_{11} & E_{12} \\ E_{21} & E_{22} \end{pmatrix}$ is positive, where E_{ij} is the matrix whose (i,j)-entry is 1, otherwise 0 ;

     Let $h_1, h_2 \in \mathbb{C}^p$. Then,

     $$\left\langle \begin{pmatrix} h_1 \\ h_2 \end{pmatrix}, \begin{pmatrix} E_{11} & E_{12} \\ E_{21} & E_{22} \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} h_1 \\ h_2 \end{pmatrix}, \begin{pmatrix} E_{11}h_1 + E_{12}h_2 \\ E_{21}h_1 + E_{22}h_2 \end{pmatrix} \right\rangle$$
     $$= \langle e_1 \otimes h_1 + e_2 \otimes h_2, e_1 \otimes (E_{11}h_1 + E_{12}h_2) + e_2 \otimes (E_{21}h_1 + E_{22}h_2) \rangle$$
     $$= \langle h_1, E_{11}h_1 + E_{12}h_2 \rangle \langle h_2, E_{21}h_1 + E_{22}h_2 \rangle$$
     $$= \langle h_1, e_1 \rangle \langle h_2, e_2 \rangle \langle e_1, h_1 \rangle \langle e_2, h_2 \rangle$$
     $$= \langle h_1, e_1 \rangle \langle h_2, e_2 \rangle \overline{\langle h_1, e_1 \rangle \langle h_2, e_2 \rangle}$$
     $$= |\langle h_1, e_1 \rangle \langle h_2, e_2 \rangle|^2 \geq 0.$$

   - $\Phi^{(2)}(E) = \begin{pmatrix} E_{11} & E_{21} \\ E_{12} & E_{22} \end{pmatrix}$ is not positive :

     $$\Phi^{(2)}(E) \begin{pmatrix} e_2 \\ -e_1 \end{pmatrix} = \begin{pmatrix} E_{11} & E_{21} \\ E_{12} & E_{22} \end{pmatrix} \begin{pmatrix} e_2 \\ -e_1 \end{pmatrix} = - \begin{pmatrix} e_2 \\ -e_1 \end{pmatrix},$$

which implies that -1 is an eigenvalue of $\Phi^{(2)}(E)$.

2.4 Partial trace

Recall that if $X \in M_m$ and $Y \in M_n$, then

- $M_m \otimes M_n \simeq M_m(M_n) \simeq M_{mn}$,
- $X \otimes Y = [x_{ij}Y] \in M_m \otimes M_n \simeq M_{mn}$,
- $\mathrm{Tr}(X \otimes Y) = x_{11}\mathrm{Tr}(Y) + x_{22}\mathrm{Tr}(Y) + \cdots + x_{nn}\mathrm{Tr}(Y) = \mathrm{Tr}(X)\mathrm{Tr}(Y)$
- Whenever $dim(\mathcal{H}_A) < \infty$ and $dim(\mathcal{H}_B) < \infty$, then $\mathcal{B}(\mathcal{H}_A) \otimes \mathcal{B}(\mathcal{H}_B) \simeq \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$. That is, if $Z \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$, then we can write $Z = \sum_i X_i \otimes Y_i$ for some $X_i \in \mathcal{B}(\mathcal{H}_A), Y_i \in \mathcal{B}(\mathcal{H}_B)$.

From the above facts, we define the **partial trace** as an operator.

Definition 2.4.1 (Partial Trace)

1. $\mathrm{Tr}_A : \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{B}(\mathcal{H}_B) \simeq \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B) \longrightarrow \mathbb{C} \otimes \mathcal{B}(\mathcal{H}_B) \simeq \mathcal{B}(\mathcal{H}_B)$, defined by $\mathrm{Tr}_A(X \otimes Y) = \mathrm{Tr}(X)Y$ is the **partial trace** *with respect to* the space $\mathcal{H}_A$.
2. $\mathrm{Tr}_B : \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{B}(\mathcal{H}_B) \simeq \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B) \longrightarrow \mathcal{B}(\mathcal{H}_A) \otimes \mathbb{C} \simeq \mathcal{B}(\mathcal{H}_A)$, defined by $\mathrm{Tr}_B(X \otimes Y) = \mathrm{Tr}(Y)X$ is the **partial trace** *with respect to* the space $\mathcal{H}_B$.

2.5 Bra-ket notation on a Hilbert space

All elements $|u\rangle$ of $\mathcal{H}$ are called **ket vectors**, and all elements $\langle v|$ of the dual $\mathcal{H}^*$ are called **bra vectors**. The bra-ket $\langle v|u\rangle$ denotes the sesquilinear

form, which is linear in $|u\rangle$ and anti-linear in $\langle v|$. Therefore $|u\rangle$ and $\langle u|$ can be represented as the following column and row vectors with complex entries, respectively:

$$|u\rangle = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix}, \langle u| = \begin{bmatrix} \overline{z_1} & \overline{z_2} & \dots & \overline{z_n} \end{bmatrix}$$

From the above concepts, we can know the bra vectors are exactly the *adjoint* of of ket vectors.(That is, $\langle u| \equiv |u\rangle^*$)

There are some results of bra-ket vectors and we arrange them below:

- For vectors $|u\rangle, |v\rangle$ and operator X, $\langle v|Xu\rangle = \langle v|X|u\rangle = \langle X^*v|u\rangle$.
- If $|u\rangle \in \mathcal{H}_1$ and $|v\rangle \in \mathcal{H}_2$ are vectors, then $|u\rangle\langle v|$ is an operator $\mathcal{H}_2 \to \mathcal{H}_1$ with $(|u\rangle\langle v|)\,|w\rangle = \langle v|w\rangle|u\rangle$
- $\mathrm{Tr}[|u\rangle\langle v|] = \langle v|u\rangle$

Chapter 3

Quantum viewpoint

3.1 Postulates in Quantum Mechanics

Postulate 1 *Each isolated physical system is associated to a Hilbert space $\mathcal{H}$, and each unit vector in $\mathcal{H}$ represents a possible state.(We will call unit vectors pure state, $\mathcal{H}$ a state space later).*

Postulate 2 *Every quantum state is interpreted by Measurement system, which is a class of operators $\{M_i\}_i$ between Hilbert spaces, $M_i : \mathcal{H}_A \longrightarrow \mathcal{H}_B$, where the index i is one of the measurement outcomes.(We will define Measurement system explicitly in Section 3.3.)*

The probability that we observe the outcome i after the input state $|\psi\rangle$ is measured(mapped) by the measurement $\{M_i\}$, is given by $p_i = \|M_i|\psi\rangle\|^2$ (hence, we have $\sum_i p_i = 1$)

If we observe the outcome i, then $|\psi\rangle$ changes to the state $\frac{M_i|\psi\rangle}{\|M_i|\psi\rangle\|}$, that is,

$$\underline{input} : |\psi\rangle \in \mathcal{H}_s, \ \ \underline{output} : \left\{ \frac{M_i|\psi\rangle}{\|M_i|\psi\rangle\|} \right\}_i \ \text{with} \ \underline{probability} \ \ p_i = \|M_i|\psi\rangle\|^2 .$$

Thus, after the observation, we will have a mixed one of states $\left\{ \frac{M_i|\psi\rangle}{\|M_i|\psi\rangle\|} \right\}_i$ with $\frac{M_i|\psi\rangle}{\|M_i|\psi\rangle\|}$ occuring with probabilities $p_i = \|M_i|\psi\rangle\|^2$.

Postulate 3 *Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be Hilbert spaces for two quantum systems. Then, the Hilbert space corresponding to the composite system AB is denoted by $\mathcal{H}_{AB}$. We use the tensor product to express $\mathcal{H}_{AB}$, that is,*

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B.$$

Hence, if dim($\mathcal{H}_A$) = d_A and dim($\mathcal{H}_B$) = d_B, then dim($\mathcal{H}_{AB}$) = $d_A d_B$.

Lemma 3.1.1 *[6] Let $T \in \mathcal{B}(\mathcal{H})$ be hermitian. If $\langle\psi|T\psi\rangle = 0$ for all $|\psi\rangle \in \mathcal{H}$ with $\||\psi\rangle\| = 1$, then $T = 0$.*

Observation 1 *Keeping in mind that quantum mechanics is inherently probabilistic, we consider a quantum experiment with at most k possible outcomes. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be Hilbert spaces, and let $M_i \in \mathcal{B}(\mathcal{H}_\mathcal{A}, \mathcal{H}_\mathcal{B}), 1 \leq i \leq k$. If the system is in state $|\psi\rangle \in \mathcal{H}_A, \||\psi\rangle\| = 1$ before we measure, then we have*

$$\langle\psi|\psi\rangle = 1 = \sum_{i=1}^{k} p_i = \sum_{i=1}^{k} \|M_i|\psi\rangle\|^2 = \sum_{i=1}^{k} \langle\psi|M_i^* M_i\psi\rangle.$$

By the previous lemma, we conclude that $\sum_{i=1}^{k} M_i^* M_i = I$.

3.2 Quantum states

Definition 3.2.1 Let $\mathcal{H}$ be a Hilbert space. If ρ is a positive operator of unit trace on $\mathcal{H}$, then it is called **density operator**(or **state**), and we denote the set of all density operators on $\mathcal{H}$ by $\mathcal{S}(\mathcal{H})$.

Proposition 3.2.2 *Let $\mathcal{P}$ be the set of all positive linear functionals φ on $\mathcal{B}(\mathcal{H})$ with $\|\varphi\| = 1$, and define a map $\Phi : \mathcal{S}(\mathcal{H}) \longrightarrow \mathcal{P}$ as $\Phi(\rho) = \varphi_\rho$, where $\varphi_\rho(A) = Tr(\rho A)$ for all $A \in \mathcal{B}(\mathcal{H})$. Then the following statements hold :*

(1) Φ is bijective.

(2) $\rho \in \mathcal{S}(\mathcal{H})$ is positive if and only if φ_ρ is positive.

(3) $Tr(\rho) = 1$ if and only if $\|\varphi_\rho\| = 1$.

Proof. (1) (Injectivity) If we assume that $\varphi_\rho = 0$, then for all $A \in \mathcal{B}(\mathcal{H})$, $0 = \varphi_\rho(A) = \mathrm{Tr}(\rho A)$. If we specially pick A as a positive operator, then we choose operators X and Y such that $\rho = X^*X$ and $A = Y^*Y$. Thus, we have

$$0 = \mathrm{Tr}(X^*XY^*Y) = \mathrm{Tr}(YX^*XY^*) = \mathrm{Tr}((XY^*)^*XY^*),$$

which implies that XY^*=0 and hence $\rho A = 0$. Putting $A = I$ shows that $\rho = 0$. (Surjectivity) Let $\varphi \in \mathcal{P}$. If we set $\rho = \sum_{i,j} \varphi(E_{ij})E_{ji}$, then it is easy to check $\Phi(\rho) = \varphi$.

(2) ($\Longrightarrow$) For all $h \in \mathcal{H}$, suppose that $\mathrm{Tr}(h^*\rho h) = \langle \rho h, h\rangle \geq 0$, and $A \in \mathcal{B}(\mathcal{H})_+$. By the Spectral Decomposition, $\rho = \sum_{i=1}^{K} \lambda_i |\psi\rangle\langle\psi|$ for some $\lambda_i > 0, |\psi_i\rangle \in \mathcal{H}$. Since trace is a linear map, it is enough to show that it holds for the case $\rho = |\psi\rangle\langle\psi|$. But the positivity of A implies that $\mathrm{Tr}(\rho A) = \mathrm{Tr}(|\psi\rangle\langle\psi|A) = \langle A\psi|\psi\rangle \geq 0$, which shows that φ_ρ is positive.

($\Longleftarrow$) Assume that φ_ρ is positive. For any $|\psi\rangle \in \mathcal{H}$, let $A = |\psi\rangle\langle\psi|$. Then clearly A is positive. Thus, $\langle\rho\psi, \psi\rangle = \langle\psi, \rho\psi\rangle = \mathrm{Tr}(|\rho\psi\rangle\langle\psi|) = \mathrm{Tr}(\rho A) \geq 0$.

(3) Note that $\mathcal{B}(\mathcal{H})$ is a C^*-algebras. Since φ_ρ is a non-zero positive linear functional on $\mathcal{B}(\mathcal{H})$, $\|\varphi_\rho\| = \varphi_\rho(I)$. ([2])
($\Longrightarrow$) If we assume that $\mathrm{Tr}(\rho) = 1$, then $\varphi_\rho(I) = \mathrm{Tr}(\rho I) = \mathrm{Tr}(\rho) = 1$.
($\Longleftarrow$) Obviously, $1 = \|\varphi_\rho\| = \varphi_\rho(I) = \mathrm{Tr}(\rho)$.

□

Remark 3.2.3 From the above proposition, we have an alternative definition of *density operator*, that is, a positive linear functional on $\mathcal{B}(\mathcal{H})$ with unit norm.

3.3 Measurement system and distinguishable states

Definition 3.3.1 (Measurement System) A finite family $\{M_i : 1 \leq i \leq k\}$ of operators $M_i : \mathcal{H} \longrightarrow \mathcal{K}$ is called a **measurement system** if the equality $\sum_{i=1}^{k} M_i^* M_i = I$ holds. If $\mathcal{H} = \mathcal{K}$, then we say that $\{M_i\}$ is a measurement system *on* $\mathcal{H}$.

Definition 3.3.2 (Perfectly Distinguishable States) A collection of states $\{|\psi_1\rangle, \cdots, |\psi_N\rangle\} \subseteq \mathcal{H}$ is said to be **perfectly distinguishable** if there exists a measurements system $\{M_i : 1 \leq i \leq k\}$, $k \geq N$ on $\mathcal{H}$ such that $\|M_i|\psi_j\rangle\|^2 = \delta_{ij}$ for $i, j \in \{1, \cdots, N\}$, where δ_{ij} is defined as

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

Theorem 3.3.3 *A collection of states* $\{|\psi_1\rangle, \cdots, |\psi_N\rangle\} \subseteq \mathcal{H}$ *is perfectly distinguishable if and only if* $|\psi_i\rangle \perp |\psi_j\rangle$ *for all* $i \neq j$.

Proof. ($\Longrightarrow$) Assume that there is a measurement system $\{M_k : 1 \leq k \leq N\}$ satisfying that $\|M_k|\psi_i\rangle\|^2 = \delta_{ki}$ for $k, i \in \{1, \cdots, N\}$. $|\psi_j\rangle = \alpha|\psi_i\rangle + \beta|\eta\rangle$, where $|\eta\rangle \perp |\psi_i\rangle, \||\eta\rangle\| = 1$. Since $1 = \||\psi_j\rangle\|^2 = |\alpha|^2 + |\beta|^2$, we have $1 = \|M_j(|\psi_j\rangle)\|^2 = \|M_j(\alpha|\psi_i\rangle + \beta|\eta\rangle)\|^2 = |\beta|^2 \|M_j(|\eta\rangle)\|^2 \leq |\beta|^2 \||\eta\rangle\| = |\beta|^2 \leq 1$, which implies that $|\beta| = 1$ and $\alpha = 0$, hence $|\psi_i\rangle \perp |\psi_j\rangle$.
($\Longleftarrow$) Let M_i be the orthogonal projection onto the subspace span$\{|\psi_i\rangle\}$. Then $M_i = M_i^* = M_i^* M_i$ for $i = 1, 2, \cdots, N$, and $\sum_{i=1}^N M_i^* M_i$ is the orthogonal projection onto span$\{|\psi_1\rangle, \cdots, |\psi_N\rangle\}$. Let M_0 be the orthogonal projection onto $(\text{span}\{|\psi_1\rangle, \cdots, |\psi_N\rangle\})^\perp$. Clearly, $\sum_{i=0}^N M_i^* M_i = \sum_{i=1}^N M_i = I$. In addition, $M_k(|\psi_i\rangle) = \delta_{ki}|\psi_i\rangle$ for all $k, i \in \{1, \cdots, N\}$, which shows that $\|M_k(|\psi_i\rangle)\|^2 = \delta_{ki}$ for $k, i \in \{1, \cdots, N\}$. □

Definition 3.3.4 Let $\mathcal{H}$ be a Hilbert space and let $\{\rho_1, \ldots, \rho_d\} \subseteq \mathcal{B}(\mathcal{H})$.
If there exists a mesurement system $\{M_1, \ldots, M_k\}$, $k \geq d$, such that $\text{Tr}(M_i \rho_j M_i^*)$ $= \delta_{ij}$, then the operators $\{\rho_1, \ldots, \rho_d\}$ are said to be **perfectly distinguishable**.

As the Theorem 3.3.3, we can derive an equivalent condition for perfectly distinguishability for operators. Firstly, We introduce two lemmas without proofs.(For the proofs, see [8].)

Lemma 3.3.5 *If* $\rho \in M_n$ *with* $\rho \geq 0$ *and* $Tr(\rho) = 0$, *then* $\rho = 0$.

Lemma 3.3.6 *Let* $\rho_1, \rho_2 \in M_n$ *be positive semi-definite operators. Then the followings are equivalent:*

(1) $\langle \rho_1, \rho_2 \rangle = 0$.

(2) $\rho_1 \rho_2 = 0$.

(3) $ran(\rho_1) \perp ran(\rho_2)$: The ranges of the states ρ_1, ρ_2 are orthogonal.

Theorem 3.3.7 *A collection of density operators $\{\rho_1, \ldots, \rho_d\} \subseteq M_n$ is perfectly distinguishable if and only if the ranges of the operators $\{\rho_i\}$ are mutually orthogonal.*

Proof. ($\Longrightarrow$) Assume that there exists a measurement system $\{V_i\} \subseteq M_n$ such that $\mathrm{Tr}(V_i \rho_j V_i^*) = \delta_{ij}$. For i, j, $i \neq j$, we have

$$\mathrm{Tr}(V_i^* V_i \rho_j) = \mathrm{Tr}(V_i \rho_j v_i^*) = 0.$$

Since both $V_i^* V_i$ and ρ_j are positive semi-definite, we have $V_i^* V_i \rho_j = 0$ by the Lemma 3.3.6. Also we have

$$\mathrm{Tr}(\rho_i V_i^* V_i) = \mathrm{Tr}(V_i \rho_i V_i^*) = 1 = \mathrm{Tr}(\rho_i),$$

which implies that $\mathrm{Tr}[\rho_i(I - V_i^* V_i)] = 0$. Note that $I - V_i^* V_i = \sum_{k \neq i} V_k^* V_k$ is obviously positive semi-definite operator. Using the Lemma 3.3.6 again, we have

$$\rho(I - V_i^* V_i) = 0 \Longleftrightarrow \rho = \rho V_i^* V_i$$

Hence, for $i \neq j$, we have

$$\rho_i \rho_j = \rho_i V_i^* V_i \rho_j = \rho_i \cdot 0 = 0.$$

This result implies that $ran(\rho_i) \perp ran(\rho_j)$, by Lemma 3.3.6
($\Longleftarrow$) Let us assume that $ran(\rho_i) \perp ran(\rho_j)$ for $i \neq j$. If we set V_i is the orthogonal projection onto $ran(\rho_i)$, then $\sum_{i=1}^{d} V_i$ is a projection hence so is $V_{i+1} := I - \sum_{i=1}^{d} V_i$. Then, we have

$$\sum_{i=1}^{d+1} V_i^* V_i = \sum_{i=1}^{d+1} V_i = I,$$

which implies that $\{V_i\}$ is a measurement system. Note that

$$\mathrm{Tr}(V_i\rho_j V_i^*) = \begin{cases} 0 & \text{if } i \neq j \\ \mathrm{Tr}(V_i\rho_i) = \mathrm{Tr}(\rho_i) = 1 & \text{if } i = j \end{cases}$$

which is the result we want. □

3.4 Pure states, mixed states

Note that $\mathcal{S}(\mathcal{H})$ is a convex set. To see this, let $\rho, \sigma \in \mathcal{S}(\mathcal{H})$, and let $\lambda \in \mathbb{R}, 0 \leq \lambda \leq 1$. Then, the linearity of trace map forces $\mathrm{Tr}(\lambda\rho + (1-\lambda)\sigma)$ $= \lambda\mathrm{Tr}(\rho) + (1-\lambda)\mathrm{Tr}(\sigma) = \lambda + (1-\lambda) = 1$, which means that $\lambda\rho + (1-\lambda)\sigma \in \mathcal{S}(\mathcal{H})$. Since the trace map is continuous, $\mathcal{S}(\mathcal{H})$ is a compact set, so there exist extreme points of $\mathcal{S}(\mathcal{H})$, which is defined as following :

Definition 3.4.1 Let X be a convex set. An element $x \in X$ is called an **extreme point** of X provided that if $x = ty + (1-t)z$ for $y, z \in X$, $0 < t < 1$, then $x = y = z$.

Lemma 3.4.2 *If $A \in \mathcal{S}(\mathcal{H})$ has rank 1, then $A^2 = A$.*

Proof. Note that any rank 1 operator is of the form $|u\rangle\langle v|$. Thus, if $A = |u\rangle\langle v|$, then it is followed that

$$\begin{aligned} A^2 &= (|u\rangle\langle v|)(|u\rangle\langle v|) = (\langle v|u\rangle)|u\rangle\langle v| \\ &= (\langle v|u\rangle)A = A, \end{aligned}$$

where the last equality follows from the assumption $A \in \mathcal{S}(\mathcal{H})$. □

Proposition 3.4.3 *A density operator $\rho \in \mathcal{S}(\mathcal{H})$ is an extreme point if and only if ρ has rank 1.*

Proof. ($\Longrightarrow$) Suppose that ρ is an extreme point of $\mathcal{S}(\mathcal{H})$. By the Spectral Theorem, $\rho = \sum_{i=1}^{k} \lambda_i |v_i\rangle\langle v_i|$, where $\lambda_i > 0$. Obviously, $\{\lambda_i\}$ satisfies that $\sum_{i=1}^{k} \lambda_i = 1$ because ρ is an element of $\mathcal{S}(\mathcal{H})$.

$$\begin{aligned}\rho &= \sum_{i=1}^{k} \lambda_i |v_i\rangle\langle v_i| = \lambda_1 |v_1\rangle\langle v_1| + \lambda_2 |v_2\rangle\langle v_2| + \cdots + \lambda_k |v_k\rangle\langle v_k| \\ &= \lambda_1 |v_1\rangle\langle v_1| + (1-\lambda_1)\left(\frac{\lambda_2}{1-\lambda_1} |v_2\rangle\langle v_2| + \cdots + \frac{\lambda_2}{1-\lambda_1} |v_k\rangle\langle v_k| \right)\end{aligned}$$

Since both $|v_1\rangle\langle v_1|$ and $\frac{\lambda_2}{1-\lambda_1}|v_2\rangle\langle v_2| + \cdots + \frac{\lambda_2}{1-\lambda_1}|v_k\rangle\langle v_k|$ are elements of $\mathcal{S}(\mathcal{H})$. From the definition of the extreme point, $\rho = |v_1\rangle\langle v_1| = \frac{\lambda_2}{1-\lambda_1}|v_2\rangle\langle v_2| + \cdots + \frac{\lambda_2}{1-\lambda_1}|v_k\rangle\langle v_k|$. Therefore, $\rho = |\psi\rangle\langle\psi|$ for some $\psi \in \mathcal{H}$, $\||\psi\rangle\| = 1$, which is an rank 1 operator.
($\Longleftarrow$) Let A be a rank 1 operator in $\mathcal{S}(\mathcal{H})$, and assume that $A = \lambda\rho + (1-\lambda)\sigma$ with $\lambda \in (0,1)$, $\rho, \sigma \in \mathcal{S}(\mathcal{H})$. Since A is a density operator by the Proposition 3.4.3, we have $A^2 = A$. Hence, $A = A^2 = \lambda^2\rho^2 + \lambda(1-\lambda)(\rho\sigma + \sigma\rho) + (1-\lambda)^2\sigma^2$. Then we have the following long inequalities :

$$\begin{aligned}1 = \mathrm{Tr}(A) &= \mathrm{Tr}\big(\lambda^2\rho^2 + \lambda(1-\lambda)(\rho\sigma + \sigma\rho) + (1-\lambda)^2\sigma^2\big) \\ &= \lambda^2\mathrm{Tr}(\rho^2) + \lambda(1-\lambda)\big(\mathrm{Tr}(\rho\sigma) + \mathrm{Tr}(\sigma\rho)\big) + (1-\lambda)^2\mathrm{Tr}(\sigma^2) \\ &\leq \lambda^2\mathrm{Tr}(\rho^2) + \lambda(1-\lambda)\{2\sqrt{(\mathrm{Tr}(\rho^2)\mathrm{Tr}(\sigma^2)}\} + (1-\lambda)^2\mathrm{Tr}(\sigma^2) \\ &\leq \lambda^2\mathrm{Tr}(\rho^2) + \lambda(1-\lambda)\{(\mathrm{Tr}(\rho^2) + \mathrm{Tr}(\sigma^2)\} + (1-\lambda)^2\mathrm{Tr}(\sigma^2) \\ &= \lambda\mathrm{Tr}(\rho^2) + (1-\lambda)\mathrm{Tr}(\sigma^2) \\ &\leq \lambda\mathrm{Tr}(\rho) + (1-\lambda)\mathrm{Tr}(\sigma) = 1.\end{aligned}$$

Here, the first inequality is derived by the *Schwarz* inequality, the second one by *Arithmetic*$-$*Geometric* inequality, and the last one is easily derived by the fact that $\rho, \sigma \in \mathcal{S}(\mathcal{H})$. But these inequalities is actually an equality equal to 1, hence by the condition of eqaulities in *Schwarz* inequality and

Arithmetic − Geometric inequality, we have $\rho = c\sigma$ for some $c \in \mathbb{C}$. The fact $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ shows that $c = 1$. Therefore we conclude that $A = \rho = \sigma$. □

Definition 3.4.4 The extreme points of $\mathcal{S}(\mathcal{H})$ is called an **pure states**.

Remark 3.4.5 Up to multiplication by a scalar of unit modulus, the unit vector $|v\rangle$ is uniquely determined by the pure state $|v\rangle\langle v|$ and hence we often refer to $|v\rangle$ itself as the *pure state*. Also, an operator $|v\rangle\langle v|$ of unit trace, is usually called the density operator corresponding to the state $|v\rangle$.

Definition 3.4.6 An **ensemble of states**(or **mixed state**) is a finite collection $\{\psi_i, p_i : 1 \leq i \leq N\}$ of states $|\psi_i\rangle \in \mathcal{B}(\mathcal{H})$ with probabilities p_i.

Definition 3.4.7 Given an ensemble $\{\psi_i, p_i : 1 \leq i \leq N\}$, the matrix

$$\rho = \sum_{j=1}^{k} p_j |\psi_j\rangle\langle\psi_j|$$

is called a **density matrix** of the ensemble. (We also often call ρ **mixed state** in duplicate.)

Note that the density matrix $\rho = \sum_{j=1}^{k} p_j |\psi_j\rangle\langle\psi_j|$ of a ensemble $\{\psi_i, p_i : 1 \leq i \leq N\}$ has trace 1, so that $\rho \in \mathcal{S}(\mathcal{H})$, but not rank 1 operator. Thus the element of $\mathcal{S}(\mathcal{H})$, which is not the extreme point(rank 1 operator) of $\mathcal{S}(\mathcal{H})$ is a mixed state. We will introduce a concrete example of mixed states in Remark 3.5.5.

From the discussion following Postulate 2 in the Section 3.1, the probability of observing outcome i in a state $|\psi\rangle$ is defined by $p_i = \|M_i|\psi\rangle\|^2$,

where $\{M_i : 1 \leq i \leq N\}$ is a measurement system. Thus, the probability of observing the outcome i in an ensemble $\{\psi_i, p_i : 1 \leq i \leq N\}$ is

$$\sum_{j=1}^{k} p_j \left\| M_i|\psi_j\rangle \right\|^2 . \tag{3.1}$$

Theorem 3.4.8 *Given a measurement system $\{M_i : 1 \leq i \leq N\}$ and an ensemble $\{\psi_i, p_i : 1 \leq i \leq N\}$, the probability of observing the outcome i is $Tr\Big(M_i \rho {M_i}^*\Big)$, where $\rho = \sum_{j=1}^{k} p_j |\psi_j\rangle\langle\psi_j|$.*

Proof. From (3.1), the probability of observing the outcome i in an ensemble $\{\psi_i, p_i : 1 \leq i \leq N\}$, is

$$\sum_{j=1}^{k} p_j \left\| M_i|\psi_j\rangle \right\|^2 .$$

Simplifying this expression, we get

$$\begin{aligned}
&\sum_{j=1}^{k} p_j \left\| M_i|\psi_j\rangle \right\|^2 = \sum_{j=1}^{k} p_j (M_i|\psi_j\rangle)^* (M_i|\psi_j\rangle) \\
&= \sum_{j=1}^{k} p_j \mathrm{Tr}\left[(M_i|\psi_j\rangle)(M_i|\psi_j\rangle)^* \right] \\
&= \sum_{j=1}^{k} p_j \mathrm{Tr}\left[M_i|\psi_j\rangle\langle\psi_j|M_i^* \right] \\
&= \mathrm{Tr}\left[M_i \Big(\sum_{j=1}^{k} p_j |\psi_j\rangle\langle\psi_j| \Big) M_i^* \right]
\end{aligned}$$

□

Theorem 3.4.9 *Given an ensemble* $\{\psi_j, p_j : 1 \leq j \leq N\}$ *and a measurement system* $\{M_i : 1 \leq i \leq k\}$*, the ensemble* $\{\psi_j, p_j : 1 \leq j \leq N\}$ *becomes the ensemble* $\left\{ \frac{M_i|\psi_j\rangle}{\|M_i|\psi_j\rangle\|}, \|M_i|\psi_j\rangle\|^2 : 1 \leq i \leq k, 1 \leq j \leq N \right\}$ *after measurement.*

Proof. From the discussion preceding Postulate 3, after the input state $|\psi_j\rangle$ is measured, we have an ensemble $\left\{ \frac{M_i|\psi_j\rangle}{\|M_i|\psi_j\rangle\|}, \|M_i|\psi_j\rangle\|^2 : 1 \leq i \leq k \right\}$. Therefore if we measure the ensemble $\{\psi_j, p_j : 1 \leq j \leq N\}$, then it becomes an ensemble $\left\{ \frac{M_i|\psi_j\rangle}{\|M_i|\psi_j\rangle\|}, \|M_i|\psi_j\rangle\|^2 : 1 \leq i \leq k, 1 \leq j \leq N \right\}$. □

3.5 Entanglement in Bipartite Quantum states

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be Hilbert spaces for two quantum systems. Then, the Hilbert space corresponding to the composite system AB is denoted by $\mathcal{H}_{AB}$.

Consider the case in classical probability theory. If X_1 and X_2 are sample spaces for two experiments, then the sample space for the joint experiment is the Cartesian product $X_1 \times X_2$. Similarly, we use the tensor product to express $\mathcal{H}_{AB}$, that is, $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. Hence, if $\dim(\mathcal{H}_A) = d_A$ and $\dim(\mathcal{H}_B) = d_B$, then $\dim(\mathcal{H}_{AB}) = d_A d_B$. Also, it is obvious that whenever $|u\rangle \in \mathcal{H}_A$, and $|v\rangle \in \mathcal{H}_B$, then $|u\rangle \otimes |v\rangle \in \mathcal{H}_{AB}$. The tensor symbol is simply often omitted($|u\rangle|v\rangle$ or $|uv\rangle$), and the elements of $\mathcal{H}_{AB}$ are denoted as linear combinations of $|u\rangle|v\rangle$.

Let us assume that $\{|e_1^A\rangle, \cdots, |e_n^A\rangle\}$ and $\{|f_1^B\rangle, \cdots, |f_m^B\rangle\}$ form orthonormal bases for $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Then, the vectors $\{|e_i^A\rangle|f_j^B\rangle\}$ constitute an orthonormal basis for $\mathcal{H}_{AB}$. Once bases for two Hilbert spaces is fixed, then we often, more simply, denoted $|e_i^A\rangle|f_j^B\rangle$ by $|i\rangle|j\rangle \equiv |ij\rangle$. Similarly, we denote the composite system associated with $\mathcal{H}_{A_1}, \mathcal{H}_{A_2}, \cdots, \mathcal{H}_{A_N}$

as $\mathcal{H}_{A_1A_2\cdots A_N} = \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \cdots \otimes \mathcal{H}_{A_N}$, and the basis of such composite system are denoted by $|ijk\cdots\rangle \equiv |e_i^{A_1}\rangle \otimes |f_j^{A_2}\rangle \otimes |g_k^{A_3}\rangle \otimes \cdots$.

Now, consider the situation satisfying the following conditions:

- $\mathcal{H}_A$ and $\mathcal{H}_B$ are the Hilbert spaces for Alice's system, Bob's system, respectively.
- $\{X_k\}$ and $\{Y_k\}$ are measurement systems on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively.

Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ with $\||\psi\rangle\| = 1$. If $p_A(k)$ and $p_B(l)$ denote the probability that Alice gets outcome k in the combined lab and the probability that Bob gets outcome l in the combined lab, respectively, then

$$p_A(k) = \|(X_k \otimes I)|\psi\rangle\|^2 \quad \textit{and} \quad p_B(l) = \|(I \otimes Y_l)|\psi\rangle\|^2 .$$

If Alice has outcome k, the state changes to $\frac{(X_k\otimes I)|\psi\rangle}{\|(X_k\otimes I)|\psi\rangle\|}$. Similarly, if Bob has outcome l, then the state becomes $\frac{(I\otimes Y_l)|\psi\rangle}{\|(I\otimes Y_l)|\psi\rangle\|}$. The **joint probability** of getting outcome k for Alice and outcome l for Bob given by

$$p_{A,B}(k,l) = \|(X_k \otimes Y_l)|\psi\rangle\|^2 .$$

Additionally, we introduce the notion of conditional probabilities in the quantum setting. The **conditional probability** given that Alice got outcome k, Bob gets outcome l is given by

$$p(B = l|A = k) = \frac{\|(I \otimes Y_l)(X_k \otimes I)|\psi\rangle\|^2}{\|(X_k \otimes I)|\psi\rangle\|^2} = \frac{p(B = l, A = k)}{p(A = k)}.$$

The state is $\frac{(X_k\otimes I)|\psi\rangle}{\|(X_k\otimes I)|\psi\rangle\|}$ under the assumption Alice has already got her outcome k. Thus the probability of observing outcome l for Bob can be computed as in the usual definition probability. (Here, we used the notation $A = k$ to indicate "A gets the outcome k".)

Example 3.5.1 Consider the two-dimensional complex Hilbert space $\mathbb{C}^2$. This corresponds to a **one-qubit system** in quantum information theory. Then two vectors in $\mathbb{C}^2$ which form a basis of $\mathbb{C}^2$ are normally denoted as

$$|0\rangle = \begin{bmatrix} 0 \\ \\ 1 \end{bmatrix}, |1\rangle = \begin{bmatrix} 1 \\ \\ 0 \end{bmatrix}$$

The n-fold tensor product space $(\mathbb{C}^2)^{\otimes n}$ is the n-**qubit** Hilbert space. The basis elements of $(\mathbb{C}^2)^{\otimes n}$ is written in terms of binary strings, as $|x_1 x_2 \cdots x_n\rangle$, where $x_i \in \{0, 1\}$.

Definition 3.5.2 Let $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$. Then the states ρ_A and ρ_B, defined as $\rho_A = \mathrm{Tr}_B[\rho_{AB}]$ and $\rho_B = \mathrm{Tr}_A[\rho_{AB}]$ are called the **reduced states**(or **marginal states**) on $\mathcal{H}_A$ and $\mathcal{H}_B$.

Remark 3.5.3 By the definition, ρ_A is obtained by tracing out over an orthonormal basis in $\mathcal{H}_B$, hence ρ_A is an operator on $\mathcal{H}_A$. To see its direct computation, let $|u\rangle, |v\rangle \in \mathcal{H}_A$. Then, we can easily show that $\langle v|\rho_A|u\rangle = \sum_j \langle v|\langle f_j|\rho_{AB}|u\rangle|f_j\rangle$, for any orthonormal basis $\{|f_j\rangle\}$ for $\mathcal{H}_B$. Similarly, given $|u'\rangle, |v'\rangle \in \mathcal{H}_B$, we have $\langle v'|\rho_B|u'\rangle = \sum_i \langle e_i|\langle v'|\rho_{AB}|e_i\rangle|u'\rangle$ for any orthonormal basis $\{|e_i\rangle\}$ for $\mathcal{H}_A$.

Example 3.5.4 We shall show that the reduced states ρ_A, ρ_B of the density operator $\rho_{AB} = |\psi\rangle\langle\psi|$ corresponding to the pure state $|\psi\rangle = \sum_{k=1}^r \lambda_k |\phi_k^A\rangle|\psi_k^B\rangle$, are given by

$$\rho_A = \sum_{k=1}^r \lambda_k^2 |\phi_k^A\rangle\langle\phi_k^A|;$$

$$\rho_B = \sum_{k=1}^r \lambda_k^2 |\psi_k^B\rangle\langle\psi_k^B|.$$

Let $|u\rangle, |v\rangle \in \mathcal{H}_A$ be given. Then

$$\begin{aligned}
\langle v|\rho_A|u\rangle &= \sum_j \langle v|\langle f_j|\rho_{AB}|u\rangle|f_j\rangle \\
&= \sum_j \langle v|\langle f_j|\left(\sum_{k=1}^{r} \lambda_k |\phi_k^A\rangle|\psi_k^B\rangle\right)\left(\sum_{i=1}^{r} \lambda_k \langle\phi_i^A|\langle\psi_i^B|\right)|u\rangle|f_j\rangle \\
&= \sum_{i,j,k} \lambda_k\lambda_i \left[(\langle v|\otimes\langle f_j|)\left(|\phi_k^A\rangle\otimes|\psi_k^B\rangle\right)\right]\left[\left(\langle\phi_i^A|\otimes\langle\psi_i^B|\right)(|u\rangle\otimes|f_j\rangle)\right] \\
&= \sum_{i,j,k} \lambda_k\lambda_i \langle v|\phi_k^A\rangle\langle f_j|\psi_k^B\rangle\langle\phi_i^A|u\rangle\langle\psi_i^B|f_j\rangle \\
&= \sum_{i,j,k} \lambda_k\lambda_i \langle f_j|\psi_k^B\rangle\langle\psi_i^B|f_j\rangle\langle v|\phi_k^A\rangle\langle\phi_i^A|u\rangle.
\end{aligned}$$

Since $\{|\psi_k\rangle\}$ is also an orthonormal basis for $\mathcal{H}_B$, we put $f_j = \psi_j^B$. Then, $\langle f_j|\psi_k^B\rangle = \delta_{jk}$, and $\langle\psi_i^B|f_j\rangle = \delta_{ij}$. Hence the right side in the last equation equals to $\sum_{k=1}^r {\lambda_k}^2\langle v|\phi_k^A\rangle\langle\phi_k^A|u\rangle = \langle v|\left(\sum_{k=1}^r {\lambda_k}^2|\phi_k^A\rangle\langle\phi_k^A|\right)|u\rangle$, which implies that $\rho_A = \sum_{k=1}^r \lambda_k^2|\phi_k^A\rangle\langle\phi_k^A|$. Similarly, we can derived ρ_B as a linear combination of density operators, $\rho_B = \sum_{k=1}^r \lambda_k^2|\psi_k^B\rangle\langle\psi_k^B|$.

Remark 3.5.5 ρ_A and ρ_B in the Example 3.5.4, which is the reduced states of a density operator associated with a pure state $|\psi\rangle \in \mathcal{H}_{AB}$ are no longer pure; They are mixed states. However, they are still density operators.

Lemma 3.5.6 *Let $\rho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$. Then, the reduced states ρ_A, ρ_B are density operators, that is,*

$$\rho_B \in \mathcal{S}(\mathcal{H}_B) \ \textit{and} \ \rho_A \in \mathcal{S}(\mathcal{H}_A)$$

Proof. Since the proof for ρ_A is similar, it is enough to show that ρ_B is a density operator. Assume that $\rho = \sum_i \sigma_i \otimes \tau_i$($\{\sigma_i\}$ and $\{\tau_i\}$ are not necessarily density operators), so that $\rho_B = \sum_i \mathrm{Tr}(\sigma_i)\tau_i$. Since ρ is a density

operator, we have

$$1 = \mathrm{Tr}(\rho) = \mathrm{Tr}\Big(\sum_i \sigma_i \otimes \tau_i\Big) = \sum_i \mathrm{Tr}(\sigma_i \otimes \tau_i) = \sum_i \mathrm{Tr}(\sigma_i)\mathrm{Tr}(\tau_i)$$
$$= \mathrm{Tr}\Big(\sum_i \mathrm{Tr}(\sigma_i)\tau_i\Big) = \mathrm{Tr}(\rho_B).$$

To show the positivity of ρ_B, let $|u\rangle \in \mathcal{H}_B$, let $\{|e_k\rangle\}$ be an orthonormal basis for $\mathcal{H}_A$, and let $w_k = |e_k\rangle \otimes |u\rangle = |e_k u\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$. Since P is positive, we have

$$\begin{aligned} 0 &\leq \sum_k \langle w_k | P w_k \rangle \\ &= \sum_k \left\langle w_k | \sum_i (\sigma_i \otimes \tau_i) w_k \right\rangle \\ &= \sum_i \sum_k (\langle e_k| \otimes \langle u|)(|\sigma_i e_k\rangle \otimes |\tau_i u\rangle) \\ &= \sum_i \left(\sum_k \langle e_k | \sigma_i e_k \rangle \right) \langle u | \tau_i u \rangle \\ &= \sum_i \mathrm{Tr}(\sigma_i) \langle u | \tau_i u \rangle \\ &= \langle u | \rho_B u \rangle , \end{aligned}$$

which follows that ρ_B is positive. □

Proposition 3.5.7 *Let $\rho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, let $\{X_k\}$ and $\{Y_l\}$ be measurement systems on $\mathcal{H}_A$ and $\mathcal{H}_B$, and let ρ_A, ρ_B be reduced state of ρ. Then*

$$p(A = k) = Tr(X_k \rho_A X_k^*) \text{ and } p(B = l) = Tr(Y_l \rho_B Y_l^*).$$

Proof. If we denote ρ as $\rho = \sum_i \sigma_i \otimes \tau_i$, then by Theorem 3.4.8,

$$\begin{aligned}
p(A=k) &= \mathrm{Tr}\left[(X_k \otimes I)\rho(X_k \otimes I)^*\right] \\
&= \sum_i \mathrm{Tr}\left[X_k \sigma_i X_k^* \otimes \tau_i\right] \\
&= \sum_i \mathrm{Tr}\left[X_k \sigma_i X_k^*\right] \mathrm{Tr}(\tau_i) = \sum_i \mathrm{Tr}(\tau_i) \mathrm{Tr}\left[X_k \sigma_i X_k^*\right] \\
&= \sum_i \mathrm{Tr}\left[X_k \left(\mathrm{Tr}(\tau_i)\sigma_i\right) X_k^*\right] \\
&= \mathrm{Tr}\left[X_k \left(\sum_i \mathrm{Tr}(\tau_i)\sigma_i\right) X_k^*\right] \\
&= \mathrm{Tr}(X_k \rho_A X_k^*).
\end{aligned}$$

Similarly for B. □

Theorem 3.5.8 (Schmidt Decomposition) *Every pure state $|\psi\rangle \in \mathcal{H}_{AB}$ can be written as*

$$|\psi\rangle = \sum_{k=1}^{r} \lambda_k |\phi_k^A\rangle |\psi_k^B\rangle$$

where

- *$\{\lambda_k\}$ satisfies $\lambda \geq 0$ and $\sum_{k=1}^r \lambda^2 = 1$.*
- *$\{|\phi_k^A\rangle\}$ and $\{|\psi_k^B\rangle\}$ are orthonormal subsets of $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively.*

Proof. Let d_A and d_B be the dimension of $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Then, in terms of the orthonormal bases for $\mathcal{H}_A$ and $\mathcal{H}_B$, we write $|\psi\rangle$ as

$$|\psi\rangle = \sum_{i=1}^{d_A} \sum_{j=1}^{d_B} a_{ij} |i_A\rangle |j_B\rangle \tag{3.2}$$

Let $A = [a_{ij}]$, and let r be the rank of A. From the Singular value decomposition, A can be written as $A = UDV^*$, where U, V are unitaries of rank d_A and d_B, respectively, and D is a diagonal matrix of rank r with non-negative real numbers λ_k on the diagonal. Therefore,

$$|\psi\rangle = \sum_{i,j,k} u_{ik}\lambda_k v_{kj}|i_A\rangle|j_B\rangle = \sum_{i,j,k} \lambda_k (u_{ik}|i_A\rangle)(v_{kj}|j_B\rangle) = \sum_{k=1}^{r} \lambda_k |\phi_k^A\rangle|\psi_k^B\rangle,$$

where $\{|\phi_k^A\rangle \equiv u_{ik}|i_A\rangle\}$ and $\{|\psi_k^B\rangle \equiv v_{kj}|j_B\rangle\}$ constitute orthonormal set in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, since both U and V are unitary. The pure condition of $|\psi\rangle$ implies that the corresponding coefficient matrix A satisfies $\sum_{i,j} |a_{ij}|^2 = 1$, which means that $\sum_{k=1}^{r} \lambda_k^2 = 1$. □

Definition 3.5.9 Let $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle \in \mathcal{H}_{AB}$ is a bipartite *pure state* with Schmidt decomposition $|\psi\rangle = \sum_{k=1}^{r} \lambda_k |\phi_k^A\rangle|\psi_k^B\rangle$.

1. The number r of non-zero coefficients λ_k is defined to be **Schmidt rank** of the state $|\psi\rangle$.

2. $|\psi\rangle$ is said to be **separable** if its Schmidt rank is 1.

3. $|\psi\rangle$ is said to be **entangled** if it is not separable, that is, its Schmidt rank is greater than 1.

4. ρ is said to be **separable** if $|\psi\rangle$ is **separable** and ρ is said to be **entangled** if $|\psi\rangle$ is **entangled**.

Example 3.5.10 If $m = \min\{d_A, d_B\}$, where d_A and d_B are dimensions of $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, then

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i_A\rangle|i_B\rangle,$$

where $\{|i_A\rangle\}$ and $\{|i_B\rangle\}$ are orthonormal bases in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, is an entangled state in $\mathcal{H}_{AB}$.
(We call it the **maximally entangled state** in $\mathcal{H}_{AB}$.)

Remark 3.5.11 Let us see how separable pure states behave in the combined system $\mathcal{H}_A \otimes \mathcal{H}_B$. We use the measurement systems $\{X_k\}$ and $\{Y_k\}$ for the $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively and assume that $|\psi\rangle$ is a pure state, that is, $|\psi\rangle = |u\rangle|v\rangle$ with $\|u\| = \|v\| = 1$. Then one has

$$p_A(k) = \|(X_k \otimes I)(|u\rangle \otimes |v\rangle)\|^2 = \|X_k|u\rangle \otimes |v\rangle\|^2 = \|X_k|u\rangle\|^2 \||v\rangle\|^2 = \|X_k|u\rangle\|^2,$$
$$p_B(l) = \|(I \otimes Y_l)(|u\rangle \otimes |v\rangle)\|^2 = \||u\rangle \otimes Y_l|v\rangle\|^2 = \||u\rangle\|^2 \|Y_l|v\rangle\|^2 = \|Y_l|v\rangle\|^2,$$

hence the joint probability becomes

$$\begin{aligned} p(A = k, B = l) &= \|(X_k \otimes Y_l)(|u\rangle \otimes |v\rangle)\|^2 \\ &= \|X_k|u\rangle \otimes Y_l|v\rangle\|^2 = \|X_k|u\rangle\|^2 \|Y_l|v\rangle\|^2 \\ &= p_A(k)p_B(l). \end{aligned}$$

Recall that in probability theory, events E_1 and E_2 are said to be independent if $\text{Prob}(E_1 \cap E_2) = \text{Prob}(E_1)\ \text{Prob}(E_2)$. Thus we conclude that $A = k$ and $B = l$ are *independent*, so that in case of separable pure states, the quantum probabilities exactly behave as independent classical probabilities.

Next, as in the Definition 3.5.9, we can define the *separability*(or *entanglement*) of mixed states. Let us assume that ρ is a mixed state on the composite system $\mathcal{H}_{AB}$. Then by the Spectral theorem, $\rho = \sum_{k=1}^N \lambda_k \rho_k$ for some N, $\{\lambda_k\}$ with $\sum_{k=1}^N \lambda_k = 1$, $\lambda_k \geq 0$ and pure states $\{\rho_k\}$ on $\mathcal{H}_{AB}$. We define the **separability** of a mixed state as the separability of each pure state ρ_k, that is,

Definition 3.5.12 Let ρ be a (mixed) state on the composite system $\mathcal{H}_{AB}$.

1. ρ is said to be **separable** if it can be written as $\rho = \sum_{k=1}^{N} \lambda_k \sigma_k \otimes \tau_k$ for some N, $\{\lambda_k\}$ with $\sum_{k=1}^{N} \lambda_k = 1$, $\lambda_k \geq 0$ and $\sigma_k \in \mathcal{S}(H_A)$, $\tau_k \in \mathcal{S}(H_B)$

2. ρ is said to be **entangled** if it is not separable.

In fact, Definition 3.5.12 is a generalization of Definition 3.5.9. To see this, assume that $|\psi\rangle$ is a pure state and $\rho = |\psi\rangle\langle\psi|$ is the density operator associated with $|\psi\rangle$. From the *Schmidt decomposition* of $|\psi\rangle$, ρ can be written as

$$\begin{aligned}\rho &= \left[\sum_{i=1}^{r} \lambda_i |\phi_i^A\rangle|\psi_i^B\rangle\right]\left[\sum_{j=1}^{r} \overline{\lambda_j}\langle\phi_j^A|\langle\psi_j^B|\right] \\ &= \sum_{i,j} \lambda_i\overline{\lambda_j}(|\phi_i^A\rangle\langle\phi_j^A|) \otimes (|\psi_i^B\rangle\langle\psi_j^B|).\end{aligned}$$

If ρ is additionally separable, then $r = 1$ so we have $\rho = (|\phi_1^A\rangle\langle\phi_1^A|) \otimes (|\psi_1^B\rangle\langle\psi_1^B|)$. Then, the next proposition supports our assertion.

Proposition 3.5.13 *Let $\rho \in \mathcal{S}(\mathcal{H}_{AB})$ be a pure state. Then the followings are equivalent.*

(1) $\rho = (|\phi_1^A\rangle\langle\phi_1^A|) \otimes (|\psi_1^B\rangle\langle\psi_1^B|)$ for some unit vectors $|\phi_1^A\rangle \in \mathcal{H}_A, |\psi_1^B\rangle \in \mathcal{H}_B$.

(2) $\rho = \sum_{i=1}^{N} \lambda_i \sigma_i \otimes \tau_i$ for some N, $\{\lambda_i\}$ with $\sum_{i=1}^{N} \lambda_i = 1$, $\lambda_i \geq 0$ and $\sigma_i \in \mathcal{S}(H_A)$, $\tau_i \in \mathcal{S}(H_B)$.

Proof. (1) $\Longrightarrow$ (2) : This is obvious if we put N=1, $\lambda_1 = 1$, $\sigma_1 = |\phi_1^A\rangle\langle\phi_1^A|$ and $\tau = |\psi_1^B\rangle\langle\psi_1^B|$.
(2) $\Longrightarrow$ (1) : Let us assume that $\rho = \sum_{i=1}^{N} \lambda_i \sigma_i \otimes \tau_i$ for some N, $\{\lambda_i\}$ with $\sum_{i=1}^{N} \lambda_i = 1$, $\lambda_i \geq 0$ and $\sigma_i \in \mathcal{S}(H_A)$, $\tau_i \in \mathcal{S}(H_B)$. Clearly, $\rho^2 =$

$\sum_{i,j} \lambda_i\lambda_j\sigma_i\sigma_j \otimes \tau_i\tau_j$. If ρ has rank 1, then by the Proposition 3.4.3, we have $\mathrm{Tr}(\rho^2) = \mathrm{Tr}(\rho) = 1$. Thus we can derive the following inequalities

$$\begin{aligned}
1 = \mathrm{Tr}(\rho^2) &= \sum_{i,j} \lambda_i\lambda_j \mathrm{Tr}(\sigma_i\sigma_j)\mathrm{Tr}(\tau_i\tau_j) \\
&\leq \sum_{i,j} \lambda_i\lambda_j \left[\mathrm{Tr}(\sigma_i^2)\mathrm{Tr}(\sigma_j^2)\mathrm{Tr}(\tau_i^2)\mathrm{Tr}(\tau_j^2)\right]^{\frac{1}{2}} \\
&= \sum_{i} \lambda_i^2 \mathrm{Tr}(\sigma_i^2)\mathrm{Tr}(\tau_i^2) \\
&\leq \sum_{i} \lambda_i^2 \mathrm{Tr}(\sigma_i)\mathrm{Tr}(\tau_i) \\
&= \sum_{i} \lambda_i^2 = 1
\end{aligned}$$

Here, the first inequality is derived by *Schwarz inequality*. Note that the inequalities are actually equalities equal to 1. Therefore, we have $\sigma_i = \sigma_j$ and $\tau_i = \tau_j$ by the condition of equality in *Schwarz inequality*. Furthermore, $\mathrm{Tr}(\sigma^2) = 1 = \mathrm{Tr}(\tau^2)$, which implies that σ and τ are pure state in each system $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Hence $\rho = |\phi_1^A\rangle\langle\phi_1^A| \otimes |\psi_1^B\rangle\langle\psi_1^B|$ for some unit vectors $|\phi_1^A\rangle \in \mathcal{H}_A$ and $|\psi_1^B\rangle \in \mathcal{H}_B$. □

3.6 Quantum channel

Definition 3.6.1 (Quantum channel) If a linear map $u : M_n \longrightarrow M_m$ is completely positive(CP) and trace-preserving(TP), then it is called a **quantum channel**(or **CPTP map**).

To investigate quantum channel, we should know equivalent condition or some property of CP and TP. So we introduce some important propositions that describe CP and TP without proofs.(For the proof, see [1] or [8])

Theorem 3.6.2 *(Choi, 1975) If $\Phi : M_n \longrightarrow M_d$ is a linear map, then the follwings are equivalent:*

(1) Φ is CP.

(2) Φ is n-positive.

(3) $P_\Phi = [\Phi(E_{ij})]_{i,j=1}^n \in M_n(M_d)$ is positive, where E_{ij} are the standard matrix units of M_n.

*(4) (**Kraus representation**) There exist $A_1, \ldots, A_r \in M_{d\times n}$ such that $\Phi(X) = \sum_{i=1}^r A_i X A_i^*$ for all $X \in M_n$.*

Proposition 3.6.3 *$\Phi : M_n \longrightarrow M_d$ is a CPTP map if and only if there exist $A_1, \ldots, A_r \in M_{d\times n}$ such that $\Phi(X) = \sum_{i=1}^r A_i X A_i^*$ for all $X \in M_n$ with $\sum_{i=1}^r A_i^* A_i = I$.*

Definition 3.6.4 Let $\Phi : M_n \longrightarrow M_d$ be a CP map.

1. The operators A_i in the Theorem 3.6.2 is called **Kraus operator**.
2. The **Choi rank**, denoted by $\mathrm{cr}(\Phi)$ is defined as $\mathrm{cr}(\Phi) = \min\{q : \Phi(X) = \sum_{i=1}^q A_i X A_i^*\}$.

Remark 3.6.5 Under the condition that Φ is CP, $\mathrm{cr}(\Phi) = \mathrm{rank}(P_\Phi)$, where P_Φ is the matrix in the Theorem 3.6.2.

Theorem 3.6.6 *[8] Let $\Phi : M_n \longrightarrow M_d$ be a CP map with cr(Φ) = r, and suppose*

$$\Phi(X) = \sum_{i=1}^{r} A_i X A_i^* = \sum_{j=1}^{m} B_i X B_i^*$$

are two Kraus representations of Φ. Then

(1) there exists $U = (u_{ij}) \in M_{m\times r}$ *with* $U^*U = I$ *such that* $B_i = \sum_{j=1}^{r} u_{ij}A_j$ *for all* i.

(2) $span\{A_1, \ldots, A_r\} = span\{B_1, \ldots, B_m\}$.

Proposition 3.6.7 *[8] Let* $\Phi : M_n \longrightarrow M_d$ *be a CPTP map defined by* $\Phi(X) = \sum_{k=1}^{N} E_i X E_i^* = \sum_{j=1}^{r} Y_l X Y_l^*$. *Then*

$$span\{E_i^* E_j : 1 \leq i, j \leq r\} = span\{Y_l^* Y_k : 1 \leq l, k \leq r\}$$

Chapter 4

Graph operator system

Graphs play an important role in Shannon's information theory. For example, the confusability graph is associated with an operator system in the work of [5] on quantum capacity, hence it is shown that Shannon's concepts have quantum interpretations with respect to these graph operator systems.

4.1 Graph operator system

Let a finite graph $G = (V, E)$, where $V = \{1, 2, \ldots, n\}$ and $E \subset V \times V$ and edges are not ordered; that is, $(i, j) \in E \implies (j, i) \in E$. Define an operator system $\mathcal{S}_G$ by

$$\mathcal{S}_G = span\{\{E_{ij} : (i, j) \in E\} \cup \{E_{ii} : 1 \leq i \leq n\}\} \subset M_n.$$

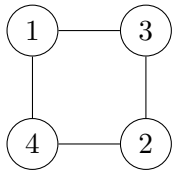
Note that $\mathcal{S}_G$ is indeed an operator system since $I = \sum_{i=1}^{n} E_{ii} \in \mathcal{S}_G$ and $\mathcal{S}_G$ is hermitian by the symmetry of the set $\{E_{ii} : 1 \leq i \leq n\} \cup \{E_{ij} : (i, j) \in E\}$.

4.2 Examples

Example 4.2.1 Suppose that $G = (V, E)$, with vertex set $V = \{1, 2, \ldots, n\}$, and edge set $E = \{(1,2), (2,3), (3,4), \ldots, (n-1, n)\}$. Then,

$$\mathcal{S}_G = \{[a_{ij}] \in M_n : a_{ij} = 0 \, for \, |i-j| > 1\} = \{tridiagonal \; matrices\}.$$

Example 4.2.2 Let G be the four-cycle graph:



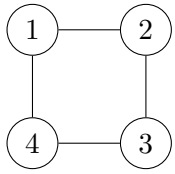
G

Then we have,

$$\mathcal{S}_G = span\{E_{11}, E_{22}, E_{33}, E_{44}, E_{13}, E_{31}, E_{32}, E_{23}, E_{24}, E_{42}, E_{41}, E_{14}\}$$

$$= \left\{ \begin{pmatrix} a & 0 & b & c \\ 0 & d & e & f \\ g & h & i & 0 \\ j & k & 0 & l \end{pmatrix} : a, \ldots, l \in \mathbb{C} \right\}.$$

But this depends on the labelling, because if we have it labelled as H:



H

Then we have

$$\mathcal{S}_H = span\{E_{11}, E_{22}, E_{33}, E_{44}, E_{12}, E_{21}, E_{23}, E_{32}, E_{34}, E_{43}, E_{41}, E_{14}\},$$

that is,

$$\mathcal{S}_H = \left\{ \begin{pmatrix} a & b & 0 & c \\ d & e & f & 0 \\ 0 & g & h & i \\ j & 0 & k & l \end{pmatrix} : a, \ldots, l \in \mathbb{C} \right\}$$

However, this is just a permutation

$$\begin{matrix} 1 \mapsto 1 \\ 2 \mapsto 3 \\ 3 \mapsto 2 \\ 4 \mapsto 4 \end{matrix}, \quad U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

so that $U\mathcal{S}_G U^* = \mathcal{S}_H$.

Chapter 5

Quantum information theory

5.1 Zero-error communication via Quantum channels

In quantum information theory, especially quantum communication, a quantum channel(CPTP) $\mathcal{T} : \mathcal{B}(\mathcal{H}_A) \longrightarrow \mathcal{B}(\mathcal{H}_B)$ means a *process*: it transmits input states $\rho \in \mathcal{B}(\mathcal{H}_A)$ to produce corresponding output states $\mathcal{T}(\rho) \in \mathcal{B}(\mathcal{H}_B)$.[7] For example, we can understand this model as an information transmission process that transmits some set of input signals from one place to another, or as a data storage scenario where some information is input into a noisy memory at one time and will be retrieved later.

Example 5.1.1 Let $\{N(y_j|x_i) \geq 0\}$ be the conditional probabilities of obtaining output $y_j \in Y$ given input $x_i \in X$ so that $\sum_j N(y_j|x_i) = 1$. Shannon described a classical channel $\mathcal{N}$ as a probability transition function $N(Y|X)$:

$$\mathcal{N} : X \longrightarrow \mathcal{P}(Y), \;\; x_i \mapsto (N(y_j|x_i))_{y_i \in Y}.$$

We can also derive a quantum channel from a classical channel as following: Let $\{|x_i\rangle\}$ and $\{|y_j\rangle\}$ be orthonormal bases for $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Then given classical channel $\mathcal{N} \equiv \{N(y_j|x_i)\}$, we can define a map $\mathcal{T}$ as

$$\mathcal{T}(\rho) = \sum_{i,j} N(y_j|x_i)|y_j\rangle\langle x_i|(\rho)|x_\rangle\langle y_j|.$$

Clearly, $\mathcal{T}$ is a CPTP map with Kraus operators $E_{ji} = \sqrt{N(y_j|x_i)}|y_j\rangle\langle x_i|$, which implies that classical channels are a special case of quantum channels.

Generally, a quantum communication protocol contains not only the action of the CPTP map but also an *encoding* map at the input side and a *decoding* map at the output. Given a set of messages $\{m = 1, 2, \ldots, q\}$, each message corresponds a quantum state $\rho_m \in \mathcal{B}(\mathcal{H}_A)$ through the encoding map, and the decoding map should extract classical information m from the output quantum state $\mathcal{T}(\rho_m) \in \mathcal{B}(\mathcal{H}_B)$.

Recall from the discussion in Section 3.1, that the outcome M of a measurement of state $\mathcal{T}(\rho_m)$ is a random variable distributed according to some classical probability distribution. We are interested in the zero-error communication, where the outcome M is equal to the original message m with probability 1. Eventually, we hope to find the maximum value of of N such that $\{\rho_1, \ldots, \rho_N\} \subseteq \mathcal{S}(\mathcal{H})$ are perfectly distinguishable.(Definition 5.2.1) The following lemma shows that each ρ_i can be assumed to be pure:

Lemma 5.1.2 *Let N, N' be the maximum values of q, r respectively for which there exist two sets*

$$\{\rho_1, \ldots, \rho_q \in \mathcal{S}(\mathcal{H}) : ran\left(\mathcal{T}(\rho_m)\right) \perp ran\left(\mathcal{T}(\rho_{m'})\right),\ \forall m \neq m'\} \text{ and}$$

$$\{|\psi_1\rangle, \ldots, |\psi_r\rangle : ran\left(\mathcal{T}(|\psi_m\rangle\langle\psi_m|)\right) \perp ran\left(\mathcal{T}(|\psi_{m'}\rangle\langle\psi_{m'}|)\right),\ \forall m \neq m'\}.$$

Then, $N = N'$.

Proof. Clearly, the inequality $N \geq N'$ holds. For the converse, consider the maximal set $\{\rho_1, \ldots, \rho_N\} \subseteq \mathcal{S}(\mathcal{H})$. By the Spectral decomposition, there exist N pure states $|\varphi_1\rangle\langle\varphi_1|, \ldots, |\varphi_N\rangle\langle\varphi_N|$ such that $\mathrm{ran}(|\varphi_m\rangle\langle\varphi_m|) \subseteq \mathrm{ran}(\rho_m)$ for each m. This follows that the ranges of the states $\{|\varphi_m\rangle\langle\varphi_m|\}$ are mutually orthogonal. This shows that $N \leq N'$. □

In this section, we find the maximum number of reliable messages passing through the quantum channels. To do that, we first review the role of operator systems in the study of the zero-error communication.[5] Consider the following equivalent statements:

(1) There exists a measurement system on $\mathcal{H}_B$ such that the outcome M corresponding to $\mathcal{T}(\rho_m)$ is equal to m with probability 1.

(2) The states $\{\mathcal{T}(\rho_m)\}$ are perfectly distinguishable.(that is, there exists a measurement system $\{V_i\}$ such that $\mathrm{Tr}(V_M \mathcal{T}(\rho_m) V_M^*) = \delta_{mM}$)

(3) The range of $\{\mathcal{T}(\rho_m)\}$ are mutually orthogonal.

(4) $\mathrm{Tr}[\mathcal{T}(\rho_m)\mathcal{T}(\rho_{m'})] = 0$ for all $m \neq m'$.

We can easily check that the relation of (1) and (2) are indeed same statements. Also, Theorem 3.3.7 shows that the statement (2), (3) and (4) are indeed equivalent. If we write $\mathcal{T}$ as Kraus representation $\mathcal{T}(\rho) = \sum_i E_i \rho E_i^*$, then the last one of the above equivalent statements follows that

(5) $\sum_{i,j} \mathrm{Tr}\,(E_i \rho_m E_i^* E_i \rho_{m'} E_i^*) = 0$ for all $m \neq m'$.

Thanks to Lemma 5.1.2, we may assume that $\{\rho_m\}$ are taken as pure. If we set $\rho_m = |\psi_m\rangle\langle\psi_m|$ and $\rho_{m'} = |\psi_{m'}\rangle\langle\psi_{m'}|$ for some states $|\psi_m\rangle, |\psi_{m'}\rangle$,

then the statement (5) becomes

$$\begin{aligned}
&|\langle\psi_m|E_i^* E_j|\psi_{m'}\rangle|^2 = 0 \text{ for all } m \neq m'. \\
&\iff \langle\psi_m|E_i^* E_j|\psi_{m'}\rangle = 0 \text{ for all } m \neq m', i, j. \\
&\iff (6)\ \ \mathrm{Tr}\,[|\psi_{m'}\rangle\langle\psi_m|E_i^* E_j] = 0 \text{ for all } m \neq m', i, j.
\end{aligned}$$

Summarizing this long discussion gives a condition for the zero-error communication using the quantum channel $\mathcal{T}$ as below:

Proposition 5.1.3 *Given a quantum channel $\mathcal{T}$ with Kraus operators $\{E_i\}$, the followings are equivalent:*

(1) Zero-error communication through $\mathcal{T}$ is possible.

(2) The input states $\{|\psi_m\rangle\} \subset \mathcal{H}_A$ to the channel satisfy the following: for all $m \neq m'$, the (rank 1) operators $|\psi_{m'}\rangle\langle\psi_m| \in \mathcal{B}(\mathcal{H}_A)$ are orthogonal to the subspace

$$S := span\{E_i^* E_j : i, j\},$$

where the orthogonality defined with respect to the Hilbert-Schmidt inner product.

Remark 5.1.4 (i) With the above setting for S, it is easy to check that the following facts are true:

- $S \subseteq \mathcal{B}(\mathcal{H}_A)$.
- Every element of S is hermitian.
- $I = \sum_i E_i^* E_i \in S$.

Thus, it is shown in the Proposition 5.1.3 that a quantum channel $\mathcal{T}$ gives rise to an *operator system* S.

(ii) Although Kraus representation of $\mathcal{T}$ is not unique, Proposition 3.6.7 shows that all Kraus represenation of $\mathcal{T}$ give rise to the same span S.

(iii) ([3], [4]) As the converse of the result in (i), it turns out that every operator system can be constructed in this manner:

Given an operator system $S \subset \mathcal{B}(\mathcal{H}_A)$, there exists a CPTP map $\mathcal{T}$ with Kraus operators $\{E_i\}$ such that $S = span\{E_i^* E_j : i, j\}$.

5.2 Zero-error capacity and Lovász ϑ function

In this section, our goal is quantifying the maximum number of messages m that can be transmitted reliably through the channel $\mathcal{T}$. First, we introduce some concepts required for quantum independence number in the work of [5]

Definition 5.2.1 (Independence number) Given an operator system $S \subseteq M_n$, the **independence number**(or **one-shot zero-error capacity**) $\alpha(S)$ is defined as the maximum value of q, such that there exist states $|\psi_1\rangle, \ldots, |\psi_q\rangle$ with $|\psi_m\rangle\langle\psi_{m'}| \perp S$ for all $m \neq m'$.

Remark 5.2.2 Consider the example for the classical case. Suppose that $\mathcal{T}$ is a quantum channel constructed from the classical channel N as in the Example 5.1.1 with the Kraus operators $\{E_{ji} = \sqrt{N(y_j|x_i)}|y_j\rangle\langle x_i|\}$. Then the operator system $S_{\mathcal{T}}$ associated with $\mathcal{T}$ is given by

$$S_{\mathcal{T}} = span\{E_{kl}^* E_{ji}\} = span\left(\sqrt{N(y_k|x_l)N(y_j|x_i)}|x_l\rangle\langle y_k|y_j\rangle\langle x_i|\right)$$
$$= span\left(\sqrt{N(y_j|x_l)N(y_j|x_i)}|x_l\rangle\langle x_i|\right)$$
$$= span\left(\{|x_i\rangle\langle x_i| : i\} \cup \{|x_l\rangle\langle x_i| : \text{there exists a } j \text{ such that } N(y_j|x_l)N(y_j|x_i) \neq 0\}\right).$$

We derive naturally the concepts of *confusability graph* from the last one of the equalities.

Definition 5.2.3 (1) The **confusability graph** of a classical channel N is the graph G with vertices $x \in X$ and edges $x \sim x'$ if and only if there exists $y \in Y$ such that $N(y|x)N(y|x') \neq 0$.

(2) Let G be a graph with vertex set X, edge set E. A subset $X_0 \subseteq X$ is said to be **independent** if for any $v, w \in X_0$, $(v, w) \notin E$.

(3) we define the **independence number** $\alpha(G)$ of a graph G is the maximum value of $card(X_0)$, such that X_0 is an independent set.

Remark 5.2.4 (1) The name, *confusability graph*, is derived from the fact that the edges $x \sim x'$ of the graph correspond to confusable inputs x, x' mapped to the same output y.

(2) The operator system S corresponding to this classical quantum channel $\mathcal{T}$ carries information about the structure of the underlying graph G:

$$span\{|x\rangle\langle x'| : x = x' \text{ or } x \sim x'\}$$

More generally, every graph G gives rise to an operator system S as we defined $\mathcal{S}_G$ in the Section 4.1.

Theorem 5.2.5 *[8] Let G be a finite graph, and let $\mathcal{S}_G$ be the operator of graph defined as in the Section 4.1. Then we have*

$$\alpha(\mathcal{S}_G) = \alpha(G).$$

Via the Theorem 5.2.5, we can infer that the independence number of operator system is a generalization of the concepts of the independence number of a graph. On the other hand, since it is to hard to estimate $\alpha(S)$, we will find some upper bounds for $\alpha(S)$.

Definition 5.2.6 We define the **quantum ϑ-function** $\vartheta(S)$ as

$$\vartheta(S) = \max\{\|I + M\| : M = M^*,\ M \perp S,\ I + M \geq 0\},$$

where the norm is the operator norm.

Proposition 5.2.7 *Given an operator system S, we have*

$$\alpha(S) \leq \vartheta(S).$$

Proof. Let us assume that $\alpha(S) = N$. Then we can easily check the following observations :

- Note that the condition $|\psi_m\rangle\langle\psi_{m'}| \perp S$ in the Definition 5.2.1 implies that

$$M = \sum_{m \neq m'} |\psi_m\rangle\langle\psi_{m'}| \perp S.$$

- Since the operator $\sum_m |\psi_m\rangle\langle\psi_{m'}| + M = \sum_{m,m'} |\psi_m\rangle\langle\psi_m|$ is positive semi-definite, we have

$$I + M \geq \sum_m |\psi_m\rangle\langle\psi_{m'}| + M \geq 0.$$

Thus the M is a candidate in the definition of $\vartheta(S)$. However, from $I \in S$, the states $\{|\psi_m\rangle : m = 1, 2, \ldots, N\}$ are orthonormal. Thus, we have

$$\begin{aligned}\left\| \sum_m |\psi_m\rangle\langle\psi_m| + M \right\| &= \left\| \sum_{m,m'} |\psi_m\rangle\langle\psi_m| \right\| \\ = \left\| \left(\sum_m |\psi_m\rangle \right) \left(\sum_{m'} \langle\psi_{m'}| \right) \right\| &= \left\| \sum_m |\psi_m\rangle \right\|^2 = N,\end{aligned}$$

which implies that $\alpha(S) \leq \vartheta(S)$. □

Example 5.2.8 Consider the channel $\Phi : \mathcal{B}(\mathbb{C}^n) \longrightarrow \mathcal{B}(\mathbb{C}^{n+1})$ defined by $\phi(X) = \sum_i^{2n} A_i X A_i^*$, where

$$A_i = \frac{1}{\sqrt{2}} E_{i,i}, \;\; A_{n+i} = \frac{1}{\sqrt{2}} E_{i+1,i} \quad \text{for } 1 \leq i \leq n.$$

(Here, $E_{i,j}$ is the matrices whose (i,j)-entry is 1, otherwise 0.)
This map is written as Kruas decomposition, so indeed a quantum channel. It is easy to see that the operator system S associated with the channel is $S = \mathcal{B}(\mathbb{C}^n) = M_n$. We shall compute $\vartheta(S)$:
From the condition $M = M^*$, we have $M = UDU^*$ for some diagonal matrix $D = diag(\lambda_1, \lambda_2, \ldots, \lambda_n)$ and unitary matrix U. The condition $M \perp S$ implies that

$$\mathrm{Tr}(B^* M) = 0, \;\; \forall B \in S$$

Thus for any $B \in S$, we have

$$\mathrm{Tr}(B^* D) = \mathrm{Tr}\left[(UB^*U^*)(UDU^*)\right] = \mathrm{Tr}\left[(UB^*U^*)M\right] = 0,$$

which means $D \perp S$. Thus, $\lambda_i = 0$, $\forall i \Longleftrightarrow D = 0$. Thus M satisfying the condition in Definition 5.2.6 is only $M = 0$. Therefore, $\vartheta(S) = 1$.

Example 5.2.9 Let $\Phi(X) : \mathcal{B}(\mathcal{H}_A) \longrightarrow \mathcal{B}(\mathbb{C}^2 \otimes \mathcal{H}_A)$ be defined by

$$\Phi(X) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ & \\ 1 & 1 \end{pmatrix} \otimes X = \left[\frac{1}{\sqrt{2}} \left(\begin{array}{c} I_n \\ \hdashline I_n \end{array} \right) \right] X \left[\frac{1}{\sqrt{2}} \left(\begin{array}{c:c} I_n & I_n \end{array} \right) \right]$$

as matrices multiplication, where $n = \dim(\mathcal{H}_A)$. Since the last multiplication is a Kraus decomposition, it is a CPTP map. Clearly, the operator system S associated with the channel Φ becomes $\mathbb{C}I_n = \{\alpha I_n : \alpha \in \mathbb{C}\}$. To compute $\vartheta(S)$ as in Example 5.2.8, we should find the property of M

in the Definition 5.2.6. First, from the condition $M \perp S$, we have $\mathrm{Tr}(M) = 0$. The condition $M = M^*$ implies that we have $M = UDU^*$ for some diagonal matrix $D = diag(\lambda_1, \lambda_2, \ldots, \lambda_n)$ $(\lambda_i \in \mathbb{R})$ and unitary matrix U. Then $\sum_i^n \lambda_i = 0$. However, since the equality

$$\|I + M\| = \|I + UDU^*\| = \|U(I + D)U^*\| = \|I + D\|$$

holds, without loss of generality, we may assume that $\mathrm{M} = \mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ with $\sum_i^n \lambda_i = 0$, $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. Furthermore, the last condition $I + M \geq 0$ derives $\lambda_i \geq -1$. Theremore,

$$\vartheta(S) = \|I + M\| = 1 + \lambda_1 = 1 - \sum_{i=2}^{n} \lambda_i \leq 1 + (n-1) = n.$$

There is a property of ϑ-function:

Lemma 5.2.10 *Given operator systems S_1 and S_2,*

$$\vartheta(S_1)\vartheta(S_2) \leq \vartheta(S_1 \otimes S_2).$$

Proof. Suppose that $\vartheta(S_1) = \|I + M_1\|$ and $\vartheta(S_2) = \|I + M_2\|$ for some M_1,M_2 with $M_i \perp S_i$ and $I + M_i \geq 0$ (i =1,2). If we define M as

$$M = M_1 \otimes I_n + I_n \otimes M_2 + M_1 \otimes M_2,$$

then we have $I_{n^2} + M = (I_n + M_1) \otimes (I_n + M_2)$.(Here, n^2 and n means the size of identity operators) The construction of M implies $M \perp S_1 \otimes S_2$. Therefore, we have

$$\vartheta(S_1)\vartheta(S_2) = (\|I_n + M_1\|)\,(\|I_n + M_2\|) = \|(I_n + M_1) \otimes (I_n + M_2)\|$$
$$= \|I_{n^2} + M\| \leq \vartheta(S_1 \otimes S_2).$$

□

To see that the above inequality can hold strictly, consider the case $S = I_n \otimes \mathcal{B}(\mathbb{C}^n)$. In [5], the authors used the work of [9] to show that

$$\vartheta(I_d \otimes \mathcal{B}(\mathbb{C}^n) = d^2.$$

Then, with the Example 5.2.8 and Example 5.2.9, we conclude that the quantum ϑ-function is not multiplicative. To complement this non-multiplicativity, a modified ϑ-function which can be regarded as a completion of $\vartheta(S)$ is defined as following:

Definition 5.2.11 (Quantum Lovász ϑ-function) For any operator system S, define the quantum Lovász function as follows:

$$\tilde{\vartheta}(S) = \sup_d \vartheta(S \otimes \mathcal{B}(\mathbb{C}^d))$$

Theorem 5.2.12 *[5] Given operator systems S_1 and S_2,*

$$\tilde{\vartheta}(S_1 \otimes S_2) = \tilde{\vartheta}(S_1)\tilde{\vartheta}(S_2).$$

Definition 5.2.13 (Entanglement-Assisted Independence Number) Given an operator system $S \subseteq \mathcal{B}(\mathcal{H}_A)$, the **entanglement-assisted independence number** of S, denoted by $\tilde{\alpha}(S)$, is the maximum value of N for which there exist a Hilbert space $\mathcal{H}_C$, a density operator $\rho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_C)$, and unitaries $\{V_1, \ldots, V_N\} : \mathcal{H}_A \otimes \mathcal{H}_C \longrightarrow \mathcal{H}_A \otimes \mathcal{H}_C$ such that

$$V_m \rho V_{m'}^* \perp S \otimes \mathcal{B}(\mathcal{H}_C) \text{ for all } m \neq m'. \tag{5.1}$$

Lemma 5.2.14 *Given two Hilbert spaces H_1,H_2, if S_1 is a subspace of H_1 and S_2 is a subspace of H_2, then*

$$(S_1 \otimes S_2)^\perp = (S_1^\perp \otimes S_2) \oplus (S_1 \otimes S_2^\perp) \oplus (S_1^\perp \otimes S_2^\perp),$$

where $\oplus$ denote a direct sum.

Proof. From the elementary linear algebra, we know that

$$H_1 = S_1 \oplus S_1^\perp, \quad H_2 = S_2 \oplus S_2^\perp.$$

Thus we have

$$\begin{aligned} H_1 \otimes H_2 &= (S_1 \oplus S_1^\perp) \otimes (S_2 \oplus S_2^\perp) \\ &= (S_1 \otimes S_2) \oplus (S_1^\perp \otimes S_2) \oplus (S_1 \otimes S_2^\perp) \oplus (S_1^\perp \otimes S_2^\perp), \end{aligned}$$

and this implies that

$$(S_1 \otimes S_2)^\perp = (S_1^\perp \otimes S_2) \oplus (S_1 \otimes S_2^\perp) \oplus (S_1^\perp \otimes S_2^\perp).$$

□

By the Lemma 5.2.14, the (5.1) is equivalent to

$$V_m \rho V_{m'}^* \in S^\perp \otimes \mathcal{B}(\mathcal{H}_C) \text{ for all } m \neq m'.$$

Proposition 5.2.15 *For given operator system $S \subseteq \mathcal{B}(\mathcal{H}_A) = M_d$,*

$$\alpha(S) \leq \tilde{\alpha}(S) \leq \tilde{\vartheta}(S)$$

Proof. The first inequality is clear from their definition. For the second one, let $\tilde{\alpha}(S) = N$. Then, there exist a Hilbert space $\mathcal{H}_C$, a density operator $\rho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_C)$, and unitaries $\{V_1, \ldots, V_N\} : \mathcal{H}_A \otimes \mathcal{H}_C \longrightarrow \mathcal{H}_A \otimes \mathcal{H}_C$ such that

$$V_m \rho V_{m'}^* \in S^\perp \otimes \mathcal{B}(\mathcal{H}_C) \text{ for all } 1 \leq m \neq m' \leq N. \tag{5.2}$$

Since the (5.2) is unchanged under the rescaling ρ, without loss of generality, ρ is taken for which the largest eigenvalue of ρ is 1. ρ can be written as $\rho = |\varphi\rangle\langle\varphi| + \rho'$, where $\rho' \perp |\varphi\rangle\langle\varphi|$ and $\|\rho'\| = 1$. Define $M = \sum_{m \neq m'} V_m \rho V_{m'}^* \otimes$

$|m\rangle\langle m| \in S^{\perp}\otimes\mathcal{B}(\mathcal{H}_C)\otimes\mathcal{B}(\mathbb{C}^N) = \left(S\otimes\mathcal{B}(\mathcal{H}_C)\otimes\mathcal{B}(\mathbb{C}^N)\right)^{\perp}$. From now on, we denote I_{ABN}, I_{AB}, I_N as the identity operators on $\mathcal{H}_A\otimes\mathcal{H}_C\otimes\mathbb{C}^N$, $\mathcal{H}_A\otimes\mathcal{H}_C$, $\mathbb{C}^N$, respectively, so that $I_{ABN} = I_{AB}\otimes I_N$. Before showing $I_{ACN}+M \geq 0$, we first check that

$$I_{ABN} \geq \sum_m V_m\rho V_m^*\otimes|m\rangle\langle m|. \tag{5.3}$$

To see this, let $|x\rangle \in \mathcal{H}_A\otimes\mathcal{H}_C$ and $|y\rangle \in \mathbb{C}^N$. Since $|y\rangle = \sum_m \langle m|y\rangle|m\rangle$, we have $\langle y|y\rangle = \sum_m \|\langle m|y\rangle\|^2$. We observe that the following inequality holds:

$$\begin{aligned}
&\langle xy|I_{ABN}|xy\rangle = \langle x|x\rangle\langle y|y\rangle = \langle x|x\rangle\sum_m \|\langle m|y\rangle\|^2 \\
&= \sum_m \langle x|x\rangle\,\|\langle m|y\rangle\|^2 = \sum_m \langle x|V_mV_m^*|x\rangle\,\|\langle m|y\rangle\|^2 \\
&\geq \sum_m \langle x|V_m\rho V_m^*|x\rangle\,\|\langle m|y\rangle\|^2 \\
&= \langle xy|\left(\sum_m V_m\rho V_m^*\otimes|m\rangle\langle m|\right)|xy\rangle,
\end{aligned}$$

which implies that the inequality (5.3) indeed holds.

Thus, we have

$$\begin{aligned}
&I_{ABN}+M = I_{ABN} + \sum_{m\neq m'} V_m\rho V_{m'}^*\otimes|m\rangle\langle m'| \\
&\geq \sum_m V_m\rho V_m^*\otimes|m\rangle\langle m| + \sum_{m\neq m'} V_m\rho V_{m'}^*\otimes|m\rangle\langle m'| \\
&= \sum_{m,m'} V_m\rho V_{m'}^*\otimes|m\rangle\langle m'| \\
&= \left(\sum_m V_m\sqrt{\rho}\otimes|m\rangle\right)\left(\sum_{m'}\sqrt{\rho}V_{m'}^*\otimes\langle m'|\right)
\end{aligned}$$

$$= \left(\sum_m V_m \sqrt{\rho} \otimes |m\rangle \right) \left(\sum_m V_m \sqrt{\rho} \otimes |m\rangle \right)^* \geq 0$$

Finally, if we define $|\rho\rangle = \frac{1}{\sqrt{N}} \sum_m V_m |\varphi m\rangle$, then

$$\begin{aligned} \|I_{ABN} + M\| &\geq \left\| \left(\sum_m V_m \sqrt{\rho} \otimes |m\rangle \right) \left(\sum_m V_m \sqrt{\rho} \otimes |m\rangle \right)^* \right\| \\ &\geq \langle \phi | \left(\sum_m V_m \sqrt{\rho} \otimes |m\rangle \right) \left(\sum_m V_m \sqrt{\rho} \otimes |m\rangle \right)^* |\phi\rangle = N, \end{aligned}$$

which completes the proof. □

Also, we naturally derive some inequalities from the definitions.

Proposition 5.2.16 *Given two operator systems S_1, S_2 with $S_1 \subseteq S_2$, the following inequalities hold:*

(1) $\alpha(S_1) \geq \alpha(S_2)$

(2) $\tilde{\alpha}(S_1) \geq \tilde{\alpha}(S_2)$

(3) $\vartheta(S_1) \geq \vartheta(S_2)$

(4) $\tilde{\vartheta}(S_1) \geq \tilde{\vartheta}(S_2)$

Theorem 5.2.17 *[5] [9] Let $S \subseteq \mathcal{B}(\mathcal{H})$ be an operator system. Then the following inequalities hold:*

(1) $\vartheta(S) \leq dim(\mathcal{H})$

(2) $\tilde{\vartheta}(S) \leq (dim(\mathcal{H}))^2$

Remark 5.2.18 Sythesizing Proposition 5.2.7, Proposition 5.2.15 and Theorem 5.2.17 together follows the inequalities:

(1) $\alpha(S) \leq \vartheta(S) \leq \dim(\mathcal{H})$

(2) $\tilde{\alpha}(S) \leq \tilde{\vartheta}(S) \leq (\dim(\mathcal{H}))^2$

5.3 Examples

In this section, we compute the quantum capacities of some channels using the inequalities in the Remark 5.2.18.

Example 5.3.1 (Qubit system) From the channel Φ in Example 5.2.9 and the associated operator system S, we consider the low dimensional case, namely $\dim\mathcal{H}_A = 2$. Clearly, the operator system S becomes $\mathbb{C}I_2 = \{\alpha I_2 : \alpha \in \mathbb{C}\}$. We already know that $\alpha(S) \leq 2$ and $\tilde{\alpha}(S) \leq 4$ by the Remark 5.2.18. We first show that $\alpha(S) = 2$ and $\tilde{\alpha}(S) = 4$ which implies that that $\vartheta(S) = 2$ and $\tilde{\vartheta}(S) = 4$.

(1) We shall find two states $|v_1\rangle$, $|v_2\rangle \in \mathbb{C}^2$ such that $|v_i\rangle\langle v_j| \perp S$ for $i \neq j$. If we take $|v_i\rangle\langle v_j| = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, then for any $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in S$,

$$0 = \mathrm{Tr}\left[\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}^* |v_i\rangle\langle v_j|\right] = \mathrm{Tr}\left[\begin{pmatrix} \overline{a}\alpha & \overline{a}\beta \\ \overline{a}\gamma & \overline{a}\delta \end{pmatrix}\right],$$

which follows that $0 = \overline{a}(\alpha+\delta)$. Since $a \in \mathbb{C}$ was arbitrary, we have $\alpha+\delta = 0 \iff \delta = -\alpha$. Thus, $|v_i\rangle\langle v_j|$ is of the form $\begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix}$. Putting

$|v_i\rangle = \begin{pmatrix} x \\ y \end{pmatrix}$ and $|v_j\rangle = \begin{pmatrix} z \\ w \end{pmatrix}$ makes $|v_i\rangle\langle v_j| = \begin{pmatrix} x\overline{z} & x\overline{w} \\ y\overline{z} & y\overline{w} \end{pmatrix}$, so that

$$y\overline{w} = -x\overline{z} \tag{5.4}$$

should hold. If we put $x = z = w = \frac{1}{\sqrt{2}}$ and $y = -\frac{1}{\sqrt{2}}$, then it satisfies (5.4), which implies that $\alpha(S) = 2$.

(2) From the Remark 5.2.18, we know that $\tilde{\alpha}(S) \leq 4$. Before computing, we arrange some setting as following:

- For $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, let $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
- $\{V_1, V_2, V_3, V_4\}$ are the 1-Pauli matrices, that is,

$$V_1 = I_2, V_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, V_3 = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, V_4 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

- $\mathcal{H}_C = \mathbb{C}^2$ and $U_m = V_m \otimes I_2$ (m = 1,2,3,4).
- $\rho = \frac{1}{2}\mathrm{Tr}_C\left[|\psi\rangle\langle\psi|\right] \otimes I_2 = \frac{1}{2}\left(\frac{1}{2}I_2 \otimes I_2\right) = \frac{1}{4}I_4$.

From the above setting, $\rho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_C)$, and $\{U_m : m = 1, 2, 3, 4\}$ are

all unitary. Note that

$$U_1\rho U_2^* = (I_2 \otimes I_2)\left(\frac{1}{4}I_4\right)(V_2^* \otimes I_2) = \frac{1}{4}(V_2 \otimes I_2) \text{ and}$$

$$\begin{aligned}
&\mathrm{Tr}\left[(\alpha I_2 \otimes B)^*(U_1\rho U_2)\right] = \mathrm{Tr}\left[(\overline{\alpha}I_2 \otimes B^*)\frac{1}{4}(V_2 \otimes I_2)\right] \\
&= \frac{1}{4}\overline{\alpha}\mathrm{Tr}\left[(I_2 \otimes B^*)(V_2 \otimes I_2)\right] = \frac{1}{4}\overline{\alpha}\mathrm{Tr}\left[(I_2V_2 \otimes B^*I_2)\right] \\
&= \frac{1}{4}\overline{\alpha}\mathrm{Tr}\left[V_2\right]\mathrm{Tr}\left[B^*\right] = 0
\end{aligned}$$

for any $(\alpha I_2 \otimes B) \in \mathbb{C}I_2 \otimes \mathcal{B}(\mathcal{H}_2)$, which shows that $U_1\rho U_2^* \perp \mathbb{C}I_2 \otimes \mathcal{B}(\mathcal{H}_2)$. Similarly, we can show that $U_i\rho U_j^* \perp \mathbb{C}I_2 \otimes \mathcal{B}(\mathcal{H}_2)$ for $i \neq j$. Thus we conclude that $\tilde{\alpha}(S) = 4$.

Example 5.3.2 Let $\Phi(X) : \mathcal{B}(\mathbb{C}^2) \longrightarrow \mathcal{B}(\mathbb{C}^2)$ be defined by

$$\Phi(X) = \frac{1}{2}X + \frac{1}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} X \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = E_1XE_1^* + E_2XE_2^*,$$

where $E_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $E_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

We easily check that $E_1^*E_1 = E_2^*E_2 = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $E_1^*E_2 = E_2^*E_1 = \frac{1}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, thus we have $\sum_i E_i^*E_i = I_2$, which implies that Φ is indeed a quantum channel. The operator system S associated with the channel Φ is

$$S = span\{E_i^*E_j\} = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a, b \in \mathbb{C} \right\}.$$

As we compute $\tilde{\alpha}(S)$ in the preceding example, we first show that $\alpha(S) = 2$ which implies that $\tilde{\alpha}(S) = 2$ by Remark 5.2.18. We shall find two states $|v_1\rangle$, $|v_2\rangle \in \mathbb{C}^2$ such that $|v_i\rangle\langle v_j| \perp S$ for $i \neq j$. If we take $|v_i\rangle\langle v_j| = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, then for any $\begin{pmatrix} a & b \\ b & a \end{pmatrix} \in S$,

$$0 = \mathrm{Tr}\left[\begin{pmatrix} a & b \\ b & a \end{pmatrix}^* |v_i\rangle\langle v_j|\right] = \mathrm{Tr}\left[\begin{pmatrix} \overline{a}\alpha + \overline{b}\gamma & \overline{a}\beta + \overline{b}\delta \\ \overline{b}\alpha + \overline{a}\gamma & \overline{b}\beta + \overline{a}\delta \end{pmatrix}\right],$$

which follows that $0 = \overline{a}(\alpha + \delta) + \overline{b}(\beta + \gamma)$. Since both a and $b \in \mathbb{C}$ were arbitrary, we have

$$\begin{array}{ccc} \alpha + \delta = 0 & & \delta = -\alpha \\ \beta + \gamma = 0 & \Longleftrightarrow & \gamma = -\beta \end{array}$$

Thus, $|v_i\rangle\langle v_j|$ is of the form $\begin{pmatrix} \alpha & \beta \\ -\beta & -\alpha \end{pmatrix}$. Putting $|v_i\rangle = \begin{pmatrix} x \\ y \end{pmatrix}$ and $|v_j\rangle = \begin{pmatrix} z \\ w \end{pmatrix}$ makes $|v_i\rangle\langle v_j| = \begin{pmatrix} x\overline{z} & x\overline{w} \\ y\overline{z} & y\overline{w} \end{pmatrix}$, so that

$$y\overline{w} = -x\overline{z} \text{ and } y\overline{z} = -x\overline{w}$$

should hold. As a easy way, we put $x = y$, then $z = -w$. Thus we obtain

$$|v_1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}, |v_2\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}.$$

Since $\alpha \leq \vartheta(S) \leq \dim(\mathbb{C}^2)$, the above computation implies that $\alpha(S) = 2$.

Example 5.3.3 Let $\Phi : \mathcal{B}(\mathbb{C}^2) \longrightarrow \mathcal{B}(\mathbb{C}^3)$ be defined by

$$\Phi(X) = \sum_{i=1}^{2} E_i X E_i^*,$$

where $E_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$, $E_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$. We easily check that

$$E_1^* E_1 = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E_2^* E_2,$$

$$E_1^* E_2 = \frac{1}{2} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad E_2^* E_1 = \frac{1}{2} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

thus $\sum_{i=1}^{2} E_i^* E_i = I_2$, which implies that Φ is a quantum channel. The operator system S associated with the channel Φ is

$$S = span\{E_i^* E_j\} = \left\{ \begin{pmatrix} a & b \\ c & a \end{pmatrix} : a, b, c \in \mathbb{C} \right\}.$$

(1) $\alpha(S)$:

we shall find two orthogonal states $|v_i\rangle, |v_j\rangle$. suppose that

$$|v_i\rangle\langle v_j| = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

Then

$$|v_i\rangle\langle v_j| \perp S \Longleftrightarrow 0 = \mathrm{Tr}\left[\begin{pmatrix} a & b \\ c & a \end{pmatrix}^* |v_i\rangle\langle v_j|\right] = \overline{a}(\alpha+\delta) + \overline{b}\beta + \overline{c}\gamma$$

$$\Longleftrightarrow \alpha+\delta = 0, \beta = \gamma = 0 \ \ (\because \alpha, \beta, \gamma, \delta \in \mathbb{C} \text{ were arbitrary.})$$

Therefore, $|v_i\rangle\langle v_j|$ is of the form $\begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix}$, $\alpha \in \mathbb{C}$.

If we set $|v_i\rangle = \begin{pmatrix} x \\ y \end{pmatrix}$ and $|v_j\rangle = \begin{pmatrix} z \\ w \end{pmatrix}$ so that $|v_i\rangle\langle v_j| = \begin{pmatrix} x\overline{z} & x\overline{w} \\ y\overline{z} & y\overline{w} \end{pmatrix}$, then we have

$$x\overline{z} = -y\overline{w} \ \text{ and } \ x\overline{w} = y\overline{z}.$$

Note that the second equality equivalent to distinct four cases, that is,

$$x\overline{w} = y\overline{z} \Longleftrightarrow \begin{array}{ll} \textcircled{1}\, x = 0 = y \text{ or} & \textcircled{2}\, x = 0 = z \text{ or} \\ \textcircled{3}\, w = 0 = y \text{ or} & \textcircled{4}\, w = 0 = z \end{array}$$

But, $\textcircled{1}, \textcircled{2}, \textcircled{3}, \textcircled{4}$ mean $|v_i\rangle = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ or $|v_j\rangle = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, thus in the both two cases, $|v_i\rangle$ and $|v_j\rangle$ are not orthogonal *states*, which conclude that $\alpha(S) = 1$.

(2) $\vartheta(S)$:

By the Remark 5.2.18, $\vartheta(S) \leq 2$. Suppose that $M \in \mathcal{B}(\mathbb{C}^2)$, $M \perp S$ and

$I + M \geq 0$. Then each condition has equivalent condition as following:

$$M = M^*,\ M \perp S \Longleftrightarrow M = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}, \alpha \in \mathbb{R},$$

$$I + M \geq 0 \Longleftrightarrow \begin{pmatrix} 1+\alpha & 0 \\ 0 & 1-\alpha \end{pmatrix} \geq 0 \Longleftrightarrow -1 \leq \alpha \leq 1$$

Thus, $\vartheta(S) = \max\{\|I + M\| : M \perp S, I + M \geq 0\}$
$= \max\{1 - \alpha, 1 + \alpha : -1 \leq \alpha \leq 1\} = 2$

(3) $\tilde{\vartheta}(S)$:
Remark 5.2.18 guarantees $\tilde{\vartheta}(S) \leq 4$. Suppose that for any $d \in \mathbb{N}$, $M \in \mathcal{B}(\mathbb{C}^2) \otimes \mathcal{B}(\mathbb{C}^d)$, $M \perp S \otimes \mathcal{B}(\mathbb{C}^d)$, $M = M^*$ and $I + M \geq 0$.

- $M \perp S \otimes \mathbb{C}^d \Longleftrightarrow M \in S^\perp \otimes \mathbb{C}^d$
  $\Longleftrightarrow M = \begin{pmatrix} \sum_i a_i B_i & 0 \\ 0 & -\sum_i a_i B_i \end{pmatrix}$, $a_i \in \mathbb{C}, B_i \in \mathbb{C}^d$

- Put $B = \sum_i a_i B_i$. The condition $M = M^*$ implies $B = B^*$, so that $B = UDU^*$ for some unitary U, diagonal D. However, from the following equations

$$I + M = (I_2 \otimes U) \begin{pmatrix} I + D & 0 \\ 0 & I - D \end{pmatrix} (I_2 \otimes U^*) \text{ and}$$

$$\|I+M\| = \left\| (I_2 \otimes U) \begin{pmatrix} I+D & 0 \\ 0 & I-D \end{pmatrix} (I_2 \otimes U^*) \right\| = \left\| \begin{pmatrix} I+D & 0 \\ 0 & I-D \end{pmatrix} \right\|,$$

without loss of generality, we may assume that B is a diagonal matrix $diag(\lambda_1, \lambda_2, \ldots, \lambda_n)$ with $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$.

- $I+M \geq 0 \iff \begin{pmatrix} I+B & 0 \\ 0 & I-B \end{pmatrix} \geq 0$

  $\iff \begin{cases} 1+\lambda_i \geq 0 \\ 1-\lambda_i \geq 0 \end{cases}$, for all $i = 1, 2, \ldots, n$

  $\iff -1 \leq \lambda_i \leq 1$, for all i.

From the three initial conditions $M \perp S \otimes \mathcal{B}(\mathbb{C}^d)$, $M = M^*$ and $I+M \geq 0$, we have

$$\|I+M\| = \max\{1+\lambda_1, 1-\lambda_n : -1 \leq \lambda_i \leq 1 \text{ for all } i\} = 2,$$

which implies that $\tilde{\vartheta}(S) = \underset{d}{\mathrm{Sup}} \|I+M\| = 2$.

(4) $\tilde{\alpha}(S)$:

Related with preceding result associated with $\tilde{\vartheta}(S)$ and Remark 5.2.18, we have $\tilde{\alpha}(S) \leq \tilde{\vartheta}(S) = 2$. Take $\mathcal{H}_C = \mathbb{C}^2$, $V_1 = I_2$, $V_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and let $U_1 = V_1 \otimes I_2$ and $U_2 = V_2 \otimes I_2$, and $\rho = \frac{1}{4} I_4$. Then clearly, U_1, U_2 are unitary and ρ is a density operator on $\mathbb{C}^2 \otimes \mathcal{H}_C$. From the

simple computation, we have $U_1\rho U_2^* = U_2\rho U_1^* = \frac{1}{4}(V_2 \otimes I_2)$. Note that for any $\begin{pmatrix} a & b \\ c & a \end{pmatrix} \in S$ and $B \in \mathcal{B}(\mathcal{H}_C)$,

$$\mathrm{Tr}\left[(U_i\rho U_j^*)\left\{\begin{pmatrix} a & b \\ c & a \end{pmatrix} \otimes B\right\}^*\right] = \mathrm{Tr}\left[\frac{1}{4}(V_2 \otimes I_2)\left\{\begin{pmatrix} a & b \\ c & a \end{pmatrix}^* \otimes B^*\right\}\right]$$

$$= \frac{1}{4}\mathrm{Tr}\begin{bmatrix} \overline{a} & \overline{c} \\ V_2 & \\ \overline{b} & \overline{a} \end{bmatrix} \mathrm{Tr}\left[I_2 B^*\right] = 0,$$

which means $\tilde{\alpha}(S) = 2$.

Bibliography

[1] M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10:285–290, 2013.

[2] J. B. Conway. *A course in functional analysis*, volume 96. Springer Science & Business Media, 2013.

[3] T. S. Cubitt, J. Chen, and A. W. Harrow. Superactivation of the asymptotic zero-error classical capacity of a quantum channel. *IEEE Transactions on Information Theory*, 57(12):8114–8126, 2011.

[4] R. Duan. Super-activation of zero-error capacity of noisy quantum channels. *arXiv preprint arXiv:0906.2527*, 2009.

[5] R. Duan, S. Severini, and A. Winter. Zero-error communication via quantum channels, noncommutative graphs, and a quantum lovász number. *IEEE Transactions on Information Theory*, 59(2):1164–1174, 2012.

[6] S. Friedberg, A. Insel, and L. Spence. *Linear algebra*. Prentice Hall, New Jersey, 1997.

[7] V. P. Gupta, P. Mandayam, and V. S. Sunder. The functional analysis of quantum information theory. *arXiv:1410.7188 [quant-ph]*, 2015.

BIBLIOGRAPHY

[8] S. J. Harris and S. K. Pandey. Entanglement and non-localty. 2016.

[9] W. van Dam and P. Hayden. Renyi-entropic bounds on quantum communication. *arXiv preprint quant-ph/0204093*, 2002.

국 문 초 록

근래에 양자정보이론은 IT분야에서 중요한 도구 중 하나로써 부상하고 있다. 양자정보이론은 함수해석학과 함께 하면서 수학적으로 더 정교해졌다. 고전적 정보이론과 마찬가지로 입력 정보가 변형되는지 알아내는 것은 매우 중요한데, 특히 양자 판에서는 입력정보가 거쳐가는 어떤 양자채널들의 신뢰도를 조사하는 것은 매우 중요한 문제이다.

각각의 양자채널은 작용소계라는 수학적 구조에 대응한다는 것이 밝혀졌다. 이 논문에서는 주어진 양자채널에 대응하는 작용소계에 초점을 맞추고, 그 채널의 신뢰도를 나타내는 어떤 값들을 찾는 것을 목표한다. 하지만 때때로 채널에 따라서 그 값을 계산하는 것은 어렵다. 그래서 대안적으로 그 값의 상계를 알아본다. 5장에서는 그러한 값들을 계산하기 위하여 참고문헌 뿐만 아니라 새로운 것들에서부터 선정된 몇 가지 양자 채널의 예제들을 조사한다.

주요어휘 : 양자채널, 작용소계, 독립수, Lovász theta 함수,
학번 : 2014-21194